奥赛经典

专题研究系列

湖南省数学会
湖南师范大学数学奥林匹克研究所 组编

奥林匹克数学中的数论问题

◇沈文选 张垚 冷岗松 唐立华/编著

◆湖南师范大学出版社

图书在版编目(CIP)数据

奥林匹克数学中的数论问题/沈文选,张垚,冷岗松等编著. —长沙:湖南师范大学出版社,2009.8
(奥赛经典丛书·专题研究系列)
ISBN 978-7-5648-0036-9

Ⅰ.奥… Ⅱ.①沈…②张…③冷… Ⅲ.数论课—中学—教学参考资料 Ⅳ.O156

中国版本图书馆CIP数据核字(2009)第135407号

奥林匹克数学中的数论问题

沈文选 张 垚 冷岗松 唐立华 编著

◇组　　稿:颜李朝　廖小刚
◇责任编辑:颜李朝
◇责任校对:胡晓军
◇出版发行:湖南师范大学出版社
　　地址/长沙市岳麓山　邮编/410081
　　电话/0731.88853867　88872751　传真/0731.88872636
　　网址/http://press.hunnu.edu.cn
◇印刷:长沙化勘印刷有限公司

◇开本:730×960　1/16开
◇印张:32.5
◇插页:0.25
◇字数:700千字
◇版次:2009年8月第1版　2009年8月第1次印刷
◇书号:ISBN 978-7-5648-0036-9
◇定价:38.00元

奥赛经典

专题研究系列

奥林匹克数学中的数论问题

湖南省数学会
湖南师范大学数学奥林匹克研究所 | 组编

◇沈文选 张垚 冷岗松 唐立华/编著

湖南师范大学出版社

前 言

数学奥林匹克是起步最早、规模最大、类型多种、层次较多的一项学科竞赛活动.多年来的实践表明:这项活动可以激发青少年学习数学的兴趣,焕发青少年的学习热情,吸引他们去读一些数学小册子,促使他们寻找机会去听一些名师的讲座;这项活动可以使参与者眼界大开,跳出一个班、一个学校或一个地区的小圈子,去与其他"高手"互相琢磨,激励并培养他们喜爱有挑战性数学问题的素养与精神;这项活动可以使参与者求知欲望大增,使得他们的阅读能力、理解能力、交流能力、表达能力等诸能力与日俱进.这是一种有深刻内涵的文化现象.因此,越来越多的国家或地区除组织本国或本地区的各级各类数学奥林匹克外,还积极地参与到国际数学奥林匹克中.

我国自1986年参加国际数学奥林匹克以来,所取得成绩举世公认,十多年来一直保持世界领先的水平.其中,到2007年止,湖南的学生已取得10块金牌、3块银牌的好成绩.这优异的成绩,是中华民族精神的体现,是国人潜质的反映,是民族强盛的希望.为使我国数学奥林匹克事业可持续发展,一方面要继续吸引越来越多的青少年参与,吸引一部分数学工作者扎实地投入到这项活动中来,另一方面要深入研究奥林匹克数学的理论体系,要深入研究数学奥林匹克教育理论与教学方略,研究数学奥林匹克教育与中学数学教育的内在联系.为此,在中国数学奥林匹克委员会领导的大力支持与热情指导下,2003年,湖南师范大学成立了"数学奥林匹克研究所".研究所组建近一年来,我们几位教授都积极投身到研究所的工作中.除深入进行奥林匹克数学与数学奥林匹克教育理论研究外,还将我们多年积累的辅导讲座资料进行了全面、系统的整理,以专题讲座的形式编写成了这套专题研究丛书,分几何、代数、组合、数论、真题分析五卷.这些丰富、系统的专题知识不仅是创新地解竞赛题所不可或缺的材料,而且还可激发解竞赛题的直觉或灵感.从教育心理学角度上说,只有具备了充分的专题知识与逻辑推理知识,才能有目的、有方向、有成效地进行探究性活动.

由于这套丛书篇幅较大,2009年又进行了修订,有些部分可能整理欠完善,敬请专家、同行和读者不吝指正.

编 者

2009年8月

目 录

第一章　整数的离散性与封闭性运算

【基础知识】

1. 整数的离散性

任何两个整数 x、y 之间至少相差 1，因此有不等式：

$x<y \Leftrightarrow x+1\leqslant y$.

2. 整数的封闭性运算

任何两个整数的和、差、积以及乘方运算的结果仍为整数. 因此，这几种运算是整数的封闭性运算.

【典型例题与基本方法】

例 1　求整数 a、b、c，使它们满足条件：

$a^2+b^2+c^2+3<ab+3b+2c$.

解　由题设条件 $a^2+b^2+c^2+3<ab+3b+2c$ 及整数的离散性，有

$a^2+b^2+c^2+4\leqslant ab+3b+2c$,

上式配方变形得 $\left(a-\frac{b}{2}\right)^2+3\left(\frac{b}{2}-1\right)^2+(c-1)^2\leqslant 0$.

由于 $\left(a-\frac{b}{2}\right)^2\geqslant 0$，$\left(\frac{b}{2}-1\right)^2\geqslant 0$，$(c-1)^2\geqslant 0$，

从而 $a-\frac{b}{2}=\frac{b}{2}-1=c-1=0$.

故 $a=1$，$b=2$，$c=1$ 为所求.

例 2　（第 2 届全俄数学奥林匹克题）证明不存在整数 a，b，c，d，使得表达式 ax^3+bx^2+cx+d，当 $x=19$ 时，值为 1，当 $x=62$ 时，值为 2.

证明　设 $P(x)=ax^3+bx^2+cx+d$.

若存在满足题目要求的整数 a,b,c,d，则

$P(19)=a\cdot 19^3+b\cdot 19^2+c\cdot 19+d=1$,　①

$P(62)=a\cdot 62^3+b\cdot 62^2+c\cdot 62+d=2$.　②

②－①得

$$a(62^3-19^3)+b(62^2-19^2)+c(62-19)=1,$$

即 $43[a(62^2+62\cdot 19+19^2)+b(62+19)+c]=1$.

此式的左边是 43 的倍数，显然不能等于 1.

因而满足题目要求的整数 a，b，c，d 不存在.

例 3 （2003 年西部数学奥林匹克题）将 1、2、3、4、5、6、7、8 分别放在正方体的八个顶点上，使得每一个面上的任意三个数之和均不小于 10. 求每一面上四个数之和的最小值.

解 设某个面上的四个数 a_1、a_2、a_3、a_4 之和达到最小值，且 $a_1<a_2<a_3<a_4$. 由于小于 5 的三个不同的正整数之和最大为 9，故 $a_4\geqslant 6$，因此

$$a_1+a_2+a_3+a_4\geqslant 16.$$

如图 1-1，我们取正方体的上面依次为 1、7、3、6，下面依次为 4、8、2、5，则右侧面为 $6+3+2+5=16$，这表明 16 是可以达到的.

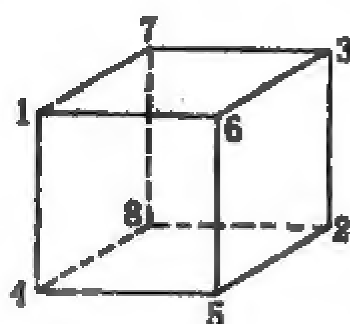


图 1-1

例 4 （2002 年女子数学奥林匹克题）求所有的正整数对 (x, y)，满足 $x^y=y^{x-y}$.

解 若 $x=1$，则 $y=1$；若 $y=1$，则 $x=1$.

若 $x=y$，则 $x^y=1$，所以 $x=y=1$.

下面讨论 $x>y\geqslant 2$ 的情形. 由题设

$$1<\left(\frac{x}{y}\right)^y=y^{x-2y},$$

所以 $x>2y$，且 x 是 y 的倍数.

设 $x=ky$，则 $k\geqslant 3$，且

$$k^y=y^{(k-2)y},$$

所以 $k=y^{k-2}$.

因为 $y\geqslant 2$，所以 $y^{k-2}\geqslant 2^{k-2}$，又用数学归纳法或二项式定理易证，当 $k\geqslant 5$ 时，$2^k>4k$，故 k 仅可能为 3 或 4.

当 $k=3$ 时，$y=3$，$x=9$；当 $k=4$ 时，$y=2$，$x=8$.

所以，所求的全部正整数对为 (1，1)，(9，3)，(8，2).

例 5 （第 5 届美国数学邀请赛题）求 k 的最大值，使 3^{11} 可以表示为 k 个连续正整数之和.

解 假设 3^{11} 表示成连续 k 个正整数之和，

$$3^{11}=(n+1)+(n+2)+\cdots+(n+k), \quad ①$$

其中 n 为非负整数，k 为正整数.

我们求满足①式的 k 的最大值.

$3^{11}=nk+\frac{k(k+1)}{2}$,

$2\cdot 3^{11}=2nk+k(k+1)$,

$2\cdot 3^{11}=k(2n+k+1)$.

显然 $k<2n+k+1$.

要使等式右边较小的因数 k 尽可能地大，又必须使 n 非负，则最大的可能是

$k=2\cdot 3^5$，$2n+k+1=3^6$.

此时可解得 $n=121$.

因此有

$3^{11}=122+123+\cdots+607$.

所求的最大的 k 为 $2\cdot 3^5=486$.

例 6 （1993 年德国数学奥林匹克题）是否存在自然数 n，使 $n!$ 的前面四位数为 1993?

解 存在.

设 $m=1000100000$，当 $k<99999$ 时，若 $(m+k)!=\overline{abcd\cdots}$，则

$(m+k+1)!=(m+k)!\times(m+k+1)$

$=\overline{abcd\cdots}\times 10001\cdots$

$=\overline{abcx\cdots}$,其中 $x=d$ 或 $d+1$.

于是,设 $m!=\overline{abcd\cdots}$,则 $(m+1)!,(m+2)!,\cdots,(m+99999)!$ 中每一个的前四位数与前一个的相等或增加 1. 而且(由于左起第五位数字增加 a),至多经过 10 个数,前四位数就需增加 1. 这样 100000 个数 $m!,(m+1)!,\cdots,(m+99999)!$ 的前四位数跑遍 10000 个值,其中必有 1993 出现.

【解题思维策略分析】

1. 逐步逼近，缩小范围

例 7 一个正整数的立方是一个四位数，这个正整数的四次方是一个六位数，这里用到的 10 个数字，恰好是 0，1，2，3，4，5，6，7，8，9 各出现一次，一个不重，一个不漏. 试求出这个正整数.

解 设这个正整数为 n. 如果 n 是一位数，那么 n^3 最多是三位数，n^4 最多是四位数，n^3 与 n^4 写在一起一定用不到 10 个数目字，所以 n 不可能是一位数.

如果 n 是三位数，即使是最小的 100，n^3 也是个七位数了，n^4 更超过七位，n^3 与 n^4 写在一起一定超过 10 个数目字，也与题设的条件不合. 因此，n 必是一个两位数.

当 n 是一个两位数时，n^4 比 n^3 至少要多一位. 所以 n^3 不能多于四位，n^4 不能

少于六位. 由于 $22^3=10648$，已经是五位数，所以 n 一定小于 22；又由于 $17^4=83521$，只是一个五位数，不到六位，所以 n 一定大于 17. 因此，n 只能是 18，19，20，21 这四个数中的某一个.

通过计算不难发现：$20^3=8000$，$19^4=130321$，$21^4=194481$，都出现数字重码现象，与题目的条件不合，应予排除. 剩下的唯一有可能合乎条件的数就只有 18 了. 由于 $18^3=5832$，$18^4=104976$，而且 10 个数目字不重不漏地出现，从而所求的正整数为 18 这个数.

类似地可求解如下答案也为 18 的问题：

问题 一个正整数分别乘以 1，2，3，4，5 后，把 5 个乘积依次排列起来，恰好出现 0，1，2，3，4，5，6，7，8，9 这 10 个数目字，一个不重，一个不漏，试求出这个正整数.

2. 提炼特征，寻求规律

例 8 设函数 f：$\mathbf{N}^+\to\mathbf{N}^+$ 是严格递增的，且对每个 $n\in\mathbf{N}^+$ 都有 $f[f(n)]=kn$. 求证：对每个 $n\in\mathbf{N}^+$，都有 $\frac{2kn}{k+1}\leqslant f(n)\leqslant\frac{(k+1)n}{2}$，$(k\in\mathbf{N}^+)$.

证明 由于 f 严格递增，且取正整数值，所以 $f(n+1)>f(n)$.

于是由整数的离散性，有 $f(n+1)\geqslant f(n)+1$.

从而，对于 $m\in\mathbf{N}^+$，有 $f(n+m)\geqslant f(n)+m$.

所以，对 $m\geqslant n$ 的正整数，有 $f(m)=f(n+m-n)\geqslant f(n)+m-n$，即有 $f(m)-m\geqslant f(n)-n$.

取 $m=f(n)$，得 $f[f(n)]-f(n)\geqslant f(n)-n$，

即有 $f(n)\leqslant\frac{1}{2}\{f[f(n)]+n\}=\frac{1}{2}(kn+n)=\frac{(k+1)n}{2}$.

用 $f(n)$ 代上式中的 n，有 $f[f(n)]\leqslant\frac{k+1}{2}\cdot f(n)$.

又 $kn=f[f(n)]\leqslant\frac{1}{2}(k+1)\cdot f(n)$，即有 $f(n)\geqslant\frac{2kn}{k+1}$.

故 $\frac{2kn}{k+1}\leqslant f(n)\leqslant\frac{(k+1)n}{2}$.

例 9 （IMO-19 试题）设 $f(n)$ 为一个在所有正整数集合 $\mathbf{N}^+$ 上有定义且在 $\mathbf{N}^+$ 上取值的函数，证明：如果对每一个正整数 n，$f(n+1)>f[f(n)]$，则对每一个 n，有 $f(n)=n$.

证明 由题设，可推测应有 $f(n+1)>f(n)$，即 $f(n)$ 单调递增. 我们放在后面再证这个结论.

这时，由 $f[f(n)]<f(n+1)$，有 $f(n)<n+1$.

注意到整数的离散性，有 $f(n)\leqslant n$.

而 $f(1)<f(2)<\cdots<f(n-1)<f(n)$，即知它们必须是前 n 个不同的正整数，故 $f(n)=n$.

下面证明 $f(n)$ 严格递增，即证 $f(1),f(2),f(3),\cdots$ 中 $f(1)$ 最小，$f(2)$ 次小，$f(3)$ 再次小，….

由题设 $f(n+1)>f[f(n)]$，知 $f(n+1)$ 不是最小的，即在 $f(2),f(3),\cdots$ 中自变量大于 1 的函数值都不是最小的，因而只有 $f(1)$ 是最小的.

再考虑 $f(2)-1,f(3)-1,\cdots$.

令 $F(n)=f(n+1)-1$，则

$F(n+1)=f(n+2)-1>f[f(n+1)]-1=f[F(n)+1]-1=F[F(n)]$.

于是，知 $F(n)$ 具有 $f(n)$ 的性质.

即知 $F(1)=f(2)-1$ 在 $f(2)-1,f(3)-1,\cdots$ 中是最小的，亦即知 $f(2)$ 在 $f(1),f(2),f(3),\cdots$ 中是次小的.

依上可证，$f(3)$ 再次小，…. 故 $f(n)$ 单调递增.

例 10 （1990 年前苏联教委推荐试题）试找出这样的 a 值，它们使得方程 $x^2-ax+9a=0$ 的根是整数.

解 设 x_1，x_2 是方程 $x^2-ax+9a=0$ 的整数根，于是由韦达定理得

$x_1+x_2=a$，

$x_1x_2=9a$.

于是 $x_1x_2=9(x_1+x_2)$，

$x_1x_2-9x_1-9x_2+81=81$，

$(x_1-9)(x_2-9)=81$.

注意到，对 81 有如下 6 种形式的因数分解：

$81=1\cdot 81=(-1)\cdot(-81)=3\cdot 27=(-3)\cdot(-27)=9\cdot 9=(-9)\cdot(-9)$.

因而可知 $a=x_1+x_2=(x_1-9)+(x_2-9)+18$，可得下面 6 个数：

$\pm 82+18$，$\pm 30+18$，$\pm 18+18$，即

$a=100$，-64，48，-12，36，0.

于是当 a 取上述 6 个整数值时，所给方程有整数根.

例 11 （第 9 届美国数学邀请赛题）有多少个实数 a，使得 $x^2+ax+6a=0$ 只有整数解.

解 设方程 $x^2+ax+6a=0$ 有整数解 m，n $(m\leqslant n)$，则有

$m+n=-a$，

$mn=6a$.

于是有 $-6(m+n)=mn$，即

$(m+6)(n+6)=36$.

因为 $36=1\cdot 36=2\cdot 18=3\cdot 12=4\cdot 9=6\cdot 6$，所以

满足 $m\leqslant n$ 的解 (m,n) 有

$(-42,-7),(-24,-8),(-18,-9),(-15,-10)$,

$(-12,-12),(-5,30),(-4,12),(-3,6),(-2,3),(0,0)$.

对应的 $a=-(m+n)$ 的值为

49，32，27，25，24，-25，-8，-3，-1，0. 共10个.

例 12 （第14届全俄数学奥林匹克题）当 $x=-1$，$x=0$，$x=1$，$x=2$ 时，多项式 $P(x)=ax^3+bx^2+cx+d$ 取整数值. 求证对于所有的整数 x，这个多项式取整数值.

证明 考虑恒等式

$$P(x)=ax^3+bx^2+cx+d$$
$$=6a\cdot\frac{(x-1)x(x+1)}{6}+2b\cdot\frac{x(x-1)}{2}+(a+b+c)x+d.$$

由于 $P(0)=d$, $P(1)=a+b+c+d$ 是整数，则 d 是整数，$a+b+c$ 是整数.

$P(-1)=2b-(a+b+c)+d$ 是整数，则 $2b$ 是整数.

$P(2)=6a+2b+2(a+b+c)+d$ 是整数，则 $6a$ 是整数.

又因为 $\frac{(x-1)x(x+1)}{6}$，$\frac{x(x-1)}{2}$ 都是整数，于是

$P(x)=6a\cdot\frac{(x-1)x(x+1)}{6}+2b\cdot\frac{x(x-1)}{2}+(a+b+c)x+d$ 对任意的整数 x，都是整数.

例 13 计算：$\sqrt{\underbrace{44\cdots4}_{2n\text{位}}+\underbrace{11\cdots1}_{n+1\text{位}}-\underbrace{66\cdots6}_{n\text{位}}}$.

解 令 $a=\underbrace{11\cdots1}_{n\text{位}}$，则

$10^n=\underbrace{99\cdots9}_{n\text{位}}+1=9a+1$,

$\underbrace{44\cdots4}_{2n\text{位}}=4a\cdot 10^n+4a=4a(9a+2)$,

$\underbrace{11\cdots1}_{n+1\text{位}}=10a+1$，$\underbrace{66\cdots6}_{n\text{位}}=6a$.

故原式 $=\sqrt{4a(9a+2)+10a+1-6a}$

$=\sqrt{(6a+1)^2}=6a+1$

$=\underbrace{66\cdots6}_{n-1\text{位}}7.$

【模拟实战】

1. (2005 年罗马利亚数学奥林匹克题) 已知 n 是一个整数，设 $p(n)$ 表示它的各位数字的乘积（用十进制表示）. (1) 求证：$p(n)\leqslant n$；(2) 求使 $10p(n)=n^2+4n-2005$ 成立的所有 n.
2. (第 48 届斯洛文尼亚数学奥林匹克题) 求方程 $\sqrt{x}+\sqrt{y}=\sqrt{2004}$ 的全部整数解.
3. (第 48 届斯洛文尼亚数学奥林匹克题) 我们在一个立方体的每个面上写一个正整数，然后，在每个顶点处再写一个数，该数等于过这个顶点的三个面上的整数的乘积. 已知该立方体各个顶点上的数字之和为 70，求该立方体各个面上的数字之和.
4. (第 4 届斯洛文尼亚数学奥林匹克题) 对每一个正整数 n，是否都存在 n 个连续的整数，使得它们的和等于 n.
5. (2003—2004 年度德国数学竞赛题) 已知数列 a_1，a_2，a_3，…定义如下：

   $a_1=1$，$a_2=1$，$a_3=2$，$a_{n+3}=\frac{1}{a_n}(a_{n+1}a_{n+2}+7)$，$n>0$.

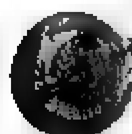
   证明：对于所有的正整数 n，a_n 是整数.
6. (2004 年克罗地亚数学竞赛题) 求所有多于两位的正整数，使得每一对相邻数字构成一个整数的平方.
7. (第 36 届奥地利数学奥林匹克题) 设 a 是整数，且 $|a|\leqslant 2005$，求使得方程组 $\begin{cases}x^2=y+a,\\ y^2=x+a\end{cases}$ 有整数解的 a 的个数.
8. (2006 年塞尔维亚和黑山队选拔赛试题) 将集合 $S=\{1, 2, \cdots, 2006\}$ 分成两个不交的子集 A 和 B，且满足

   (1) $B\in A$；

   (2) 若 $a\in A$，$b\in B$，$a+b\in S$，则 $a+b\in B$；

   (3) 若 $a\in A$，$b\in B$，$ab\in S$，则 $ab\in A$.

   求 A 中元素的数目.
9. (2003 年台湾集训题) 求所有函数 f：$\mathbf{N}\to\mathbf{N}$，对所有 m，$n\in\mathbf{N}$ 满足 $f(m^2+n^2)=f^2(m)+f^2(n)$ 且 $f(1)>0$.
10. (第 9 届中美洲及加勒比海地区数学奥林匹克题) 设 S 是有限整数集. 假设对于任两个不同的元素 p、$q\in S$，存在三个元素 a、b、$c\in S$ (a、b、c 不必不同，且 $a\neq 0$)，使得多项式 $F(x)=ax^2+bx+c$ 满足 $F(p)=F(q)=0$. 试确定 S 中元素



个数的最大值.

11. (2007年捷克 斯洛伐克 波兰数学竞赛题) 已知 $n\in\{3900, 3901, \cdots, 3909\}$. 求满足下述条件的 n：集合 $\{1, 2, \cdots, n\}$ 可分拆成若干个三元数组，且每一个数组中有一个数等于其他两数之和.

第二章　整数的相除

【基础知识】

1. 一条基本定理

定理（带余除法）　若 a，b 是两个整数，其中 $b\neq0$，则存在唯一的一对整数 q 和 r，使得

$a=bq+r$ $(0\leqslant r<|b|)$，

其中 q 称为商数，r 称为余数.

2. 定义

(1) 在上述带余除法中，当 $r=0$ 时，则称 a 能被 b 整除，或者 b 整除 a，记为 $b\mid a$，并约定 $0\mid0$. 易见当 a，b 均为正整数时，有 $b\leqslant a$.

(2) 若 $b\mid a$，则 a 叫做 b 的倍数，b 叫做 a 的约数（因数），若 $b\neq\pm1$，则 b 叫做 a 的真约数.

(3) 若 a 不能被 b 整除，则记作 $b\nmid a$.

(4) 如果 $a^t\mid b$，$a^{t+1}\nmid b$，$t\in\mathbf{N}^+$，记作 $a^t\parallel b$.

3. 欧几里得（Euclid）辗转相除法

设 a，b 是任意两个正整数，由带余除法，知

$a=bq_1+r_1(0<r_1<b)$，

$b=r_1q_2+r_2(0<r_2<r_1)$，

……

$r_{n-2}=r_{n-1}q_n+r_n(0<r_n<r_{n-1})$，

$r_{n-1}=r_nq_{n+1}+r_{n+1}(r_{n+1}=0)$，

于是 $r_n=(a,b)$.

4. 关于整除的一些简单性质

(1) $b\mid0,\pm1\mid a,a\mid a(a\neq0)$.

(2) 若 $b\mid a,a\neq0$,则 $1\leqslant|b|\leqslant|a|$.

(3) 若 $a\mid b,k\in\mathbf{Z}$,则 $a\mid kb$.

(4) 若 $a\mid b,a\mid c$,则 $a\mid(b\pm c)$.

推论 1 若 $a|b, a|(b\pm c)$，则 $a|c$.

推论 2 若 $a|b, a|c, m、n\in \mathbf{Z}$，则 $a|(mb+nc)$.

(5) 若 $a|b$，则 $a^m|b^m$.

(6) 若 $a|b, b|c$，则 $a|c$.

(7) 若 $a|c, b|c, (a,b)=1$，则 $ab|c$.

(8) 若 $a|bc, (a,b)=1$，则 $a|c$.

(9) 若 p 为素数，$p|ab$，则 $p|a$ 或 $p|b$.

推论 3 若 p 为素数，$p\mid a^m$，则 $p\mid a$.

(10) 设 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$，$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}$，则 $a\mid b\Leftrightarrow \alpha_i\leqslant\beta_i$ $(i=1, 2, \cdots, r)$.

(11) 若 $\sum\limits_{i=1}^{k}a_i=0$，$b$ 能整除 $a_1, a_2, \cdots, a_k$ 中的 $k-1$ 个，则 b 能整除另一个.

5. 几个相除结论

(1) 任何 n 个连续整数之积一定能被 n 整除.

(2) 任何 n 个连续整数之积一定能被 $n!$ 整除.

(3) $(a+b)^n$ 被 a 除的余数是 b.

【典型例题与基本方法】

例 1 （2005 年俄罗斯数学奥林匹克题）试找出不能表示为 $\dfrac{2^a-2^b}{2^c-2^d}$ 的形式的最小的正整数，其中 a、b、c、d 都是正整数.

解 所求的最小正整数是 11.

我们有：

$$1=\frac{4-2}{4-2},\ 3=\frac{8-2}{4-2},\ 5=\frac{16-1}{4-1}=\frac{2^5-2}{2^3-2},$$

$$7=\frac{16-2}{4-2},\ 9=2^3+1=\frac{2^6-1}{2^3-1}=\frac{2^7-2}{2^4-2},$$

$$2=2\cdot 1=\frac{2^3-2^2}{2^2-2},\ \cdots,\ 10=2\cdot 5=\frac{2^6-2^2}{2^3-2}.$$

假设

$$11=\frac{2^a-2^b}{2^c-2^d},$$

不失一般性，可设 $a>b$，$c>d$，记 $m=a-b$，$n=c-d$，$k=b-d$，于是得到

$$11(2^n-1)=2^k(2^m-1).$$

上式左端为奇数，因此 $k=0$. 易知 $n=1$ 不能使上式成立. 而如果 $m>n>1$，则 2^n-1 与 2^m-1 被 4 除的余数都是 3，从而上式左端被 4 除的余数为 1，右端却为 3，此为

矛盾.

例 2 (1972 年第 6 届全苏数学奥林匹克题)(1)设 a,m,n 是自然数,$a>1$. 证明:如果 a^m+1 能被 a^n+1 整除,那么 m 能被 n 整除. (2)设 a,b,m,n 是自然数,同时 a 和 b 互素,且 $a>1$. 证明:如果 a^m+b^m 能被 a^n+b^n 整除,那么 m 能被 n 整除.

证明 注意到(1)是(2)的特例,即(2)中 $b=1$ 的情形,所以我们只证明(2).

首先证明如下两个引理:

引理 1:若 $a^n+b^n \mid a^k+b^k$,$(a,b)=1$,则 $a^n+b^n \mid a^{k-n}-b^{k-n}$.

引理 2:若 $a^n+b^n \mid a^l-b^l$,$(a,b)=1$,则 $a^n+b^n \mid a^{l-n}+b^{l-n}$.

这两个引理容易由 $(a,b)=1$ 以及下面的两个恒等式得到:

$a^k+b^k=a^{k-n}(a^n+b^n)-b^n(a^{k-n}+b^{k-n})$,

$a^l-b^l=a^{l-n}(a^n+b^n)-b^n(a^{l-n}+b^{l-n})$.

设 $m=nq+r, 0\leqslant r\leqslant n$,则由引理 1,2 可知

$a^n+b^n \mid a^r+(-1)^q b^r$. ①

这是因为 r 可以从 m 减去 nq 得到.

由于 $0\leqslant |a^r+(-1)^q b^r|<a^n+b^n$,因此要满足①式,必须 $r=0$ 及 q 是奇数.

这就得到 $m=nq$,即 $n \mid m$.

例 3 (IMO-25 试题)求正整数 a,b,使之满足:

(1) $ab(a+b)$不被 7 整除;

(2) $(a+b)^7-a^7-b^7$ 被 7^7 整除.

验证你的答案.

解 我们有

$(a+b)^7-a^7-b^7=7ab(a+b)(a^2+ab+b^2)^2$.

由(1)和(2)知应有 $7^7 \mid 7ab(a+b)(a^2+ab+b^2)^2$,亦即 $7^3 \mid a^2+ab+b^2$.

下面我们来求满足

$(a+b)^2-ab=a^2+ab+b^2=7^3=343$ ①

的正整数 a,b.

由于 $0<ab\leqslant\frac{1}{4}(a+b)^2$,于是由①可得估计式

$343\leqslant(a+b)^2\leqslant457$,

解得 $19\leqslant a+b\leqslant21$.

令 $a+b=19$,由①得 $ab=18$,联立解得 $a=18$,$b=1$,容易验证,这是一对满足 (1) 和 (2) 的正整数.

例 4 (1992 年"友谊杯"国际数学竞赛题)求最大自然数 x,使得对每一个自然数 y,x 能整除 $7^y+12y-1$.

解 当 $y=1$ 时，$7^y+12y-1=18$，因此 $x\mid 18$，从而 $x\leqslant 18$.

下面用数学归纳法证明：

$18\mid 7^y+12y-1$.

当 $y=1$ 时，显然.

若 $y=k$ 时，$18\mid 7^k+12k-1$.

当 $y=k+1$ 时，

$$7^{k+1}+12(k+1)-1$$
$$=7\cdot 7^k+7\cdot 12k-7-6\cdot 12k+18$$
$$=7(7^k+12k-1)-72k+18.$$

由归纳假设

$18\mid 7^k+12k-1$,

又 $18\mid -72k+18$,

于是 $18\mid 7^{k+1}+12(k+1)-1$,

即 $y=k+1$ 时命题成立.

从而对所有的自然数 y，$18\mid 7^y+12y-1$.

于是最大的自然数 $x=18$.

例5 （IMO-39 试题）试确定使 ab^2+b+7 整除 a^2b+a+b 的全部正整数对(a,b).

解 设正整数对(a,b)满足 $ab^2+b+7\mid a^2b+a+b$，则有

$ab^2+b+7\mid a(ab^2+b+7)-b(a^2b+a+b)$，即

$ab^2+b+7\mid 7a-b^2$.

(i)当 $7a-b^2=0$，即 $7\mid b$ 时，

设 $b=7k$，则 $7a=7^2k^2$，$a=7k^2$，此时有

$a^2b+a+b=k(ab^2+b+7)$.

故$(a,b)=(7k^2,7k)$是题目的解.

(ii)当 $7a-b^2>0$ 时，有 $7a-b^2\geqslant ab^2+b+7$，

$7a>ab^2$，$b^2<7$，知 $b=1$ 或 2.

若 $b=1$，则 $a+8\mid a^2+a+1$.

设 $a+8=u$，则 $a^2+a+1=(u-8)^2+(u-8)+1=u^2-15u+59$.

由 $u\mid u^2-15u+59$，得 $u\mid 59$，

于是 $u=19$ 或 57，得 $a=11$ 或 49.

此时又得到两组解$(a,b)=(11,1)$或$(49,1)$.

若 $b=2$，则 $4a+9\mid 7a-4$.

由于 $4a+9\leqslant 7a-4<2(4a+9)$，不等式对正整数 a 不成立.

综上，解为

$(a,b)=(7k^2,7k),(11,1),(49,1),k\in \mathbf{N}^+$.

例 6 （1995 年第 21 届全俄数学奥林匹克题）是否存在这样的由正整数构成的数列：其中每个正整数都恰好出现一次，并且对任何 $k=1,2,3,\cdots$，数列中前 k 项之和都可被 k 整除?

解 我们证明这样的数列是存在的.

取 $a_1=1$. 假设已取定了数列中的前 n 项：$a_1,a_2,\cdots,a_n$. 设 m 是没有被取入的最小正整数，M 是已经被取入的最大自然数.

记 $S_k=\sum\limits_{i=1}^{k}a_i$，且设 $a_{n+1}=m[(n+2)^t-1]-S_n$，$a_{n+2}=m$，其中 t 是使得 $a_{n+1}>M$ 成立的足够大的正整数.

于是有 $S_{n+1}=S_n+a_{n+1}=m[(n+2)^t-1]$ 能被 $n+1$ 整除，且

$S_{n+2}=S_{n+1}+a_{n+2}=m(n+2)^t$ 能被 $n+2$ 整除.

只要继续这样做下去，就可使每一个自然数都在我们构造的数列中出现，且都刚好出现一次.

例 7 （CMO-11 试题）设 $S=\{1,2,\cdots,50\}$，求最小自然数 k，使 S 的任一 k 元子集中都存在两个不同的数 a 和 b，满足 $(a+b)\mid ab$.

解 设有 $a,b\in S$ 满足条件 $(a+b)\mid ab$.

记 $c=(a,b)$，于是 $a=ca_1,b=cb_1$，其中 $a_1,b_1\in \mathbf{N}$，且 $(a_1,b_1)=1$.

因而有 $c(a_1+b_1)=(a+b)\mid ab=c^2a_1b_1$，故

$(a_1+b_1)\mid ca_1b_1$.

由 $(a_1,b_1)=1$ 可知 $(a_1+b_1,a_1)=1,(a_1+b_1,b_1)=1$，故有

$(a_1+b_1)\mid c$.

由 $a\in S,b\in S$，则 $a+b\leqslant 99$，且 $c(a_1+b_1)\leqslant 99$. 从而有

$3\leqslant a_1+b_1\leqslant 9$.

由此可知，S 中满足条件 $(a+b)\mid ab$ 的不同数对共有 23 对：

当 $a_1+b_1=3$ 时，$(a,b)=(6,3),(12,6),(18,9),(24,12),(30,15),(36,18),(42,21),(48,24)$;

当 $a_1+b_1=4$ 时，$(a,b)=(12,4),(24,8),(36,12),(48,16)$;

当 $a_1+b_1=5$ 时，$(a,b)=(20,5),(40,10),(15,10),(30,20),(45,30)$;

当 $a_1+b_1=6$ 时，$(a,b)=(30,6)$;

当 $a_1+b_1=7$ 时，$(a,b)=(42,7),(35,14),(28,21)$;

当 $a_1+b_1=8$ 时，$(a,b)=(40,24)$；

当 $a_1+b_1=9$ 时，$(a,b)=(45,36)$.

令 $M=\{6,12,15,18,20,21,24,35,40,42,45,48\}$，则 $|M|=12$，且上述 23 个数对中的每一对都至少包含 M 中的 1 个元素.

因此，若令 $T=S-M$，则 $|T|=38$ 且 T 中任何两数都不满足题中要求. 可见，所求的最小自然数 $k\geqslant 39$.

注意，下列 12 个满足题中要求的数对互不相交：

$(6,3),(12,4),(20,5),(42,7),(24,8),(18,9),(40,10),(35,14),(30,15),(48,16),(28,21),(45,36)$.

对于 S 中的任一 39 元子集 R，它只比 S 少 11 个元素，而这 11 个元素至少属于上述 12 个数对中的 11 对，从而必有上述 12 对中的 1 对属于 R.

综上可知，所求的最小自然数 $k=39$.

【解题思维策略分析】

1. 善于运用带余除法

例 8 （2006 年女子数学奥林匹克题）求证：对 $i=1,2,3$，均有无穷多个正整数 n，使得 n，$n+2$，$n+28$ 中恰有 i 个可表示为三个正整数的立方和.

证明 三个整数的立方和被 9 除的余数不能为 4 或 5，这是因为整数可写为 $3k$ 或 $3k\pm1$ $(k\in\mathbf{Z})$，而

$(3k)^3=9\times 3k^3$,

$(3k\pm1)^3=9(3k^3\pm3k^2+k)\pm1$.

对 $i=1$，令 $n=3(3m-1)^3-2(m\in\mathbf{Z}^+)$，则 $n,n+28$ 被 9 除的余数分别为 4,5，故均不能表示为三个整数的立方和，而

$n+2=(3m-1)^3+(3m-1)^3+(3m-1)^3$.

对 $i=2$，$n=(3m-1)^3+222(m\in\mathbf{Z}^+)$ 被 9 除的余数为 5，故不能表示为三个整数的立方和，而

$n+2=(3m-1)^3+2^3+6^3$,

$n+28=(3m-1)^3+5^3+5^3$.

对 $i=3$，$n=216m^3(m\in\mathbf{Z}^+)$ 满足条件：

$n=(3m)^3+(4m)^3+(5m)^3$,

$n+2=(6m)^3+1^3+1^3$,

$n+28=(6m)^3+1^3+3^3$.

注 所命原题要求证明结论对 $i=0,1,2,3$ 均成立.

为降低试卷难度，去掉了 $i=0$ 的要求．以下是该情形的证明：

对 $n=9m+3$，$m\in\mathbf{Z}$，$n+2$，$n+28$ 被 9 除的余数分别为 5，4，不能表示为三个整数的立方和，若 $n=a^3+b^3+c^3$，a，b，$c\in\mathbf{Z}$，由前知 a，b，c 均为 $3k+1$ 型 $(k\in\mathbf{Z})$ 的整数．

小于 $(3N)^3$ $(N\in\mathbf{Z}^+)$ 的 $9m+3$ 型 $(k\in\mathbf{Z})$ 的正整数共 $3N^3$ 个．　　（＊）

小于 $3N$ 的 $3k+1$ 型 $(k\in\mathbf{Z})$ 的正整数有 N 个，三个这样的立方数之和的组合不超过 N^3 种，故（＊）中正整数至少有 $3N^3-N^3=2N^3$ 个不能表示为三个正整数的立方和．N 可取任意正整数，故 $i=0$ 情形得证．

例 9　（IMO－19 试题）设 a，b 是正整数，当 a^2+b^2 被 $a+b$ 除时，商为 q，余数为 r，求所有的数对 (a,b)，使 $q^2+r=1977$．

解　因为 $a^2+b^2=q(a+b)+r$，其中 $0\leqslant r<a+b$，所以 $\frac{a^2+b^2}{a+b}<q+1$．

当 $q\geqslant 45$ 时，$q^2\geqslant 2025$，$r\leqslant -48$，这与 $r>0$ 矛盾，所以 $q\leqslant 44$，并且 $\frac{a^2+b^2}{a+b}<45$．

当 $q\leqslant 43$ 时，$q^2=1849$，$r\geqslant 128$，$a+b>128$，不妨设 $a\geqslant b$，则 $a\geqslant\frac{1}{2}(a+b)$．

当 $a\leqslant\frac{2}{3}(a+b)$ 时，$b\geqslant\frac{1}{3}(a+b)$，

$$\frac{a^2+b^2}{a+b}\geqslant\frac{\left[\frac{1}{2}(a+b)\right]^2+\left[\frac{1}{3}(a+b)\right]^2}{a+b}=\frac{13}{36}(a+b).$$

因为 $(a+b)>128$，所以

$\frac{a^2+b^2}{a+b}>46$，这与 $\frac{a^2+b^2}{a+b}<45$ 矛盾．

当 $a>\frac{2}{3}(a+b)$ 时，

$$\frac{a^2+b^2}{a+b}>\frac{\left[\frac{2}{3}(a+b)\right]^2}{a+b}=\frac{4}{9}(a+b)>56,$$这与 $\frac{a^2+b^2}{a+b}<45$ 矛盾．

所以 $q>43$．

但由于 $q\leqslant 44$，故 $q=44$ 且 $r=41$，所以有

$a^2+b^2=44(a+b)+41$，即

$(a-22)^2+(b-22)^2=1009$．

解得 $\begin{cases}a_1=50,\\b_1=37;\end{cases}$　$\begin{cases}a_2=50,\\b_2=7;\end{cases}$

$\begin{cases}a_3=37,\\ b_3=50;\end{cases}$ $\begin{cases}a_4=7,\\ b_4=50.\end{cases}$

即所求的数对 (a, b) 有下列四组：

$(50, 37)$，$(50, 7)$，$(37, 50)$，$(7, 50)$.

例 10 （1994 年国家集训队选拔试题）求所有的由四个正整数 a，b，c，d 组成的数组，使数组中任意三个数的乘积除以剩下的一个数的余数都是 1.

解 首先证明 a，b，c，d 都不小于 2，且两两互素.

这是因为，由题意，有 $bcd=ka+1$，显然 $a\geqslant 2$，否则，若 $a=1$，则 bcd 除以 a 的余数是 0，与题意矛盾.

同时，a 与 b，c，d 中的任意一个都互素.

同理有 $b\geqslant 2$，$c\geqslant 2$，$d\geqslant 2$，且 a，b，c，d 两两互素.

不妨设 $2\leqslant a<b<c<d$.

由于 $a\mid bcd-1$，$b\mid acd-1$，$c\mid abd-1$，$d\mid abc-1$，从而有

$a\mid bcd-1+abc+abd+acd$，

$b\mid acd-1+abc+abd+bcd$，

$c\mid abd-1+abc+acd+bcd$，

$d\mid abc-1+abd+acd+bcd$.

由 a，b，c，d 两两互素，则有

$abcd\mid abc+abd+acd+bcd-1$，

即存在正整数 t，有

$abc+abd+acd+bcd=tabcd+1$，即

$$t+\frac{1}{abcd}=\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}<\frac{4}{a}, \quad ①$$

从而 $t<\frac{4}{a}\leqslant\frac{4}{2}=2$ ($\because a\geqslant 2$).

于是 $t=1$，$a=2$ 或 $a=3$.

当 $a=3$ 时，$b\geqslant 4$，$c\geqslant 5$，$d\geqslant 6$，则

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}\leqslant\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}<1,$$

此式与①式及 $t=1$ 矛盾.

所以必有 $a=2$. 这时①式化为

$$1+\frac{1}{2bcd}=\frac{1}{2}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d},$$

故 $$\frac{1}{2}+\frac{1}{2bcd}=\frac{1}{b}+\frac{1}{c}+\frac{1}{d}<\frac{3}{b}, \quad ②$$

因而 $\frac{1}{2}<\frac{3}{b}$，即 $b<6$.

由于 $a=2,(a,b)=1,b<6$,则 $b=3$ 或 $b=5$.

当 $a=2,b=5$ 时,有 $(a,c)=1,(a,d)=1,c\geqslant 7,d\geqslant 9$,这时有

$$\frac{1}{b}+\frac{1}{c}+\frac{1}{d}<\frac{1}{5}+\frac{1}{7}+\frac{1}{9}<\frac{1}{2},$$

与③式矛盾,即 $b\neq 5$.

于是 $b=3,c>5,d\geqslant 7$.

①式又化为

$$1+\frac{1}{6cd}=\frac{1}{2}+\frac{1}{3}+\frac{1}{c}+\frac{1}{d},故$$

$$\frac{1}{c}+\frac{1}{d}=\frac{1}{6}+\frac{1}{6cd}<\frac{2}{c}. \qquad ③$$

从而 $\frac{2}{c}>\frac{1}{6},c<12$.

由 $a=2$ 知 c 是奇数,则 $c\leqslant 11$.

由③式可求出 $d=6+\frac{35}{c-6}$. ④

$d\geqslant 7,d$ 是正整数,则 $\frac{35}{c-6}$ 是正整数,考虑到 $c\leqslant 11$,则 $1\leqslant c-6\leqslant 5$,从而只能有 $c-6=1$ 或 $c-6=5$,即

$c=7$ 或 $c=11$.

当 $c=7$ 时,由④式 $d=41$,

当 $c=11$ 时,由④式 $d=13$.

于是所求的四个数 $(a,b,c,d)=(2,3,7,11)$ 或 $(2,3,11,13)$.

2. 灵活运用整除性质

例 11 （1958 年匈牙利数学奥林匹克题）证明：如果 u 和 v 是整数，u^2+uv+v^2 能被 9 整除，那么 u 和 v 都能被 3 整除.

证明 已知表达式可化为

$$u^2+uv+v^2=(u-v)^2+3uv.$$

因为 $9\mid u^2+uv+v^2,3\mid 3uv$,于是 $3\mid (u-v)^2$,

从而 $9\mid (u-v)^2,3\mid u-v$,

于是 $9\mid 3uv$,

即 $3\mid uv$.

所以 u 和 v 至少有一个能被 3 整除.

设 $3 \mid u$，则由 $3 \mid u-v$，必有 $3 \mid v$.

于是 u 和 v 都能被 3 整除.

例 12 x，y，z 是两两不相等的整数，证明 $(x-y)^5+(y-z)^5+(z-x)^5$ 能被 $5(y-z)(z-x)(x-y)$ 整除.

证明 设 $x-y=u$，$y-z=v$，则

$z-x=-(u+v)$.

$(u+v)^5=u^5+5u^4v+10u^3v^2+10u^2v^3+5uv^4+v^5$，

从而

$$
\begin{aligned}
&u^5+v^5-(u+v)^5\\
=&-5uv(u^3+2u^2v+2uv^2+v^3)\\
=&-5uv[(u^3+v^3)+2uv(u+v)]\\
=&-5uv(u+v)(u^2+uv+v^2).
\end{aligned}
$$

于是有

$$
\begin{aligned}
&(x-y)^5+(y-z)^5+(z-x)^5\\
=&5(x-y)(y-z)(z-x)[(x-y)^2+(x-y)(y-z)+(y-z)^2]\\
=&5(x-y)(y-z)(z-x)(x^2+y^2+z^2-xy-yz-zx).
\end{aligned}
$$

因而 $(x-y)^5+(y-z)^5+(z-x)^5$ 能被 $5(x-y)(y-z)(z-x)$ 整除.

例 13 假设 a，b，c，d 是整数，且数 ac，$bc+ad$，bd 都能被某整数 u 整除，证明数 bc 和 ad 也都能被 u 整除.

证法 1 由 ac，$bc+ad$，bd 都能被 u 整除，设 u 有因子 p^r（p 为素数），则有

$$ac=p^rA, \quad ①$$

$$bc+ad=p^rB, \quad ②$$

$$bd=p^rC, \quad ③$$

其中 A，B，C 是整数.

①×③得

$(bc)(ad)=p^{2r}AC$.

因此，bc 和 ad 的分解式中必有一个 p 的指数不小于 r，不妨设 $bc=p^tD$（$t\geqslant r$，D 是整数），于是

$p^r \mid bc$.

再由②可得 $p^r \mid ad$.

于是 bc 和 ad 都能被 p^r 整除，从而 bc 和 cd 都能被 u 整除.

证法 2 考虑到等式

$(bc-ad)^2=(bc+ad)^2-4acbd$.

在等式两边同时除以 u^2 得

$$\left(\frac{bc-ad}{u}\right)^2=\left(\frac{bc+ad}{u}\right)^2-4\cdot\frac{ac}{u}\cdot\frac{bd}{u}.$$

由于 ac，bd，$bc+ad$ 都能被 u 整除，则

$$s=\frac{bc+ad}{u},\ p=\frac{ac}{u},\ q=\frac{bd}{u}$$

都是整数，即

$$\left(\frac{bc-ad}{u}\right)^2=s^2-4pq.$$

于是$\frac{bc-ad}{u}$也为整数.

令 $t=\frac{bc-ad}{u}$，于是 $t^2=s^2-4pq$，即 $s^2-t^2=4pq$，即

$$(s+t)(s-t)=4pq.$$

由于任意两个整数的和与它们的差具有相同的奇偶性，以及由 $4pq$ 是偶数可知 $s+t$与 $s-t$ 必为偶数.

于是$\frac{bc}{u}=\frac{s+t}{2}$，$\frac{ad}{u}=\frac{s-t}{2}$必为整数，即 bc 和 ad 都能被 u 整除.

3. 关注 k 个连续整数的乘积能被 k 整除

例 14 （1973 年基辅数学奥林匹克题）设 a_1，a_2，…，a_n 是自然数，它们的和能被 30 整除. 证明 $a_1^5+a_2^5+\cdots+a_n^5$ 能被 30 整除.

证明 首先证明 $30\mid a^5-a$. 由于

$$\begin{aligned}a^5-a&=a(a^2-1)(a^2+1)\\&=(a-1)a(a+1)(a^2-4+5)\\&=(a-2)(a-1)a(a+1)(a+2)+5(a-1)a(a+1).\end{aligned}$$

$a-2,a-1,a,a+1,a+2$ 是连续五个整数，它们的乘积能被 $5!=120$ 整除，因而能被 30 整除.

$a-1,a,a+1$ 是连续三个整数，它们的乘积能被 $3!=6$ 整除，因而 $5(a-1)a(a+1)$ 能被 30 整除.

于是 $30\mid a^5-a$.

从而 $30\mid\sum\limits_{i=1}^{n}(a_i^5-a_i)=\sum\limits_{i=1}^{n}a_i^5-\sum\limits_{i=1}^{n}a_i$.

又由已知 $30\mid\sum\limits_{i=1}^{n}a_i$，所以

$$30\mid\sum_{i=1}^{n}a_i^5.$$

例 15 (1989年第7届美国数学邀请赛题)如果 $a<b<c<d<e$ 是连续的正整数,$b+c+d$ 是完全平方数,$a+b+c+d+e$ 是完全立方数,那么 c 的最小值是多少?

解 因为 a,b,c,d,e 是连续的正整数,所以有

$b+c+d=3c$,

$a+b+c+d+e=5c$.

由于 $b+c+d$ 是完全平方数,$a+b+c+d+e$ 是完全立方数,所以可设

$$3c=m^2, \quad ①$$

$$5c=n^3. \quad ②$$

由①得 $3|m$,进而 $3|c$.

由②得 $5|n$,进而 $5^2|c$.

再由②得 $3^3|c$.

于是 $25\cdot 27|c$.

又 $c\geqslant 25\cdot 27=675$,

因此 c 的最小值是 675.

例 16 (1971年基辅数学奥林匹克题)证明对任意整数 n,$\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}$是整数.

证明 设 $N=\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}$.

$$N=\frac{n(n^2-1)(n^2-4)}{5}+\frac{5n^3-4n}{5}+\frac{n(n^2-1)}{3}+\frac{n}{3}+\frac{7n}{15}$$

$$=n^3+\frac{(n-2)(n-1)n(n+1)(n+2)}{5}+\frac{(n-1)n(n+1)}{3}.$$

由于 $n-2,n-1,n,n+1$ 和 $n+2$ 是五个连续整数,必有一个能被 5 整除,因此 $\frac{(n-2)(n-1)n(n+1)(n+2)}{5}$是整数.

又由于 $n-1$, n 和 $n+1$ 是三个连续整数,所以,必有一个能被 3 整除,因此 $\frac{(n-1)\ n\ (n+1)}{3}$是整数.

于是,对任意整数 n,$N=\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}$是整数.

4. 适时运用数学归纳法

例 17 (1985年保加利亚数学竞赛题) k 与 n 为正整数,证明

$$(n^4-1)(n^3-n^2+n-1)^k+(n+1)n^{4k-1}$$

能被 n^5+1 整除.

证明 对 k 使用数学归纳法.

(1) 当 $k=1$ 时，

$(n^4-1)(n^3-n^2+n-1)+(n+1)\cdot n^3$

$=n^7-n^6+n^5+n^2-n+1=(n^5+1)(n^2-n+1)$.

因而能被 n^5+1 整除.

(2)假设 $n^5+1\mid(n^4-1)(n^3-n^2+n-1)^k+(n+1)n^{4k-1}$，那么

对 $k+1$ 时，

$(n^4-1)(n^3-n^2+n-1)^{k+1}+(n+1)n^{4(k+1)-1}$

$=(n^4-1)(n^3-n^2+n-1)^k(n^3-n^2+n-1)+(n+1)n^{4k-1}n^4$

$=(n^4-1)(n^3-n^2+n-1)^k(n^3-n^2+n-1)+(n+1)n^{4k-1}(n^3-n^2+n-1)+$
$\quad(n+1)n^{4k-1}n^4-(n+1)n^{4k-1}(n^3-n^2+n-1)$

$=[(n^4-1)(n^3-n^2+n-1)^k+(n+1)n^{4k-1}](n^3-n^2+n-1)+$
$\quad(n+1)n^{4k-1}(n^4-n^3+n^2-n+1)$

$=[(n^4-1)(n^3-n^2+n-1)^k+(n+1)n^{4k-1}](n^3-n^2+n-1)+(n^5+1)n^{4k-1}$.

由归纳假设，第一项能被 n^5+1 整除，而第二项显然能被 n^5+1 整除，于是

$n^5+1\mid(n^4-1)(n^3-n^2+n-1)^{k+1}+(n+1)n^{4(k+1)-1}$.

即对 $k+1$ 命题成立.

于是对所有自然数 k，命题成立.

例 18 （1998 年第 27 届美国数学奥林匹克题）证明对任意 $n\in\mathbf{N}$，$n\geqslant2$，存在一个由 n 个整数构成的集合 S，使得对 S 中的任意两个不同的数 a 和 b，均有 $(a-b)^2\mid ab$.

证明 我们对 n 使用数学归纳法.

当 $n=2$ 时，取 $S_2=\{1,2\}$，则有 $(1-2)^2\mid1\times2$，因此，$n=2$ 时，命题成立.

假设 $n=k$ 时命题成立，即存在含有 k 个元素的集合 $S_k=\{a_1,a_2,\cdots,a_k\}$ 满足条件，对任意 $1\leqslant i\leqslant j\leqslant k$，均有 $(a_i-a_j)^2\mid a_ia_j$.

记 $A=a_1a_2\cdots a_k$，考虑如下 $k+1$ 个数：

A，$A+a_1$，$A+a_2$，$\cdots$，$A+a_k$.

由于 $[(A+a_i)-(A+a_j)]^2=(a_i-a_j)^2$，

$(A+a_i)(A+a_j)=A^2+A(a_i+a_j)+a_ia_j$.

由归纳假设及 A 的定义，有

$(a_i-a_j)^2\mid a_ia_j$，

$a_ia_j\mid A^2+A(a_i+a_j)+a_ia_j$，

因此 $[(A+a_i)-(A+a_j)]^2\mid(A+a_i)(A+a_j)$.

另一方面，$[(A+a_j)-A]^2=a_i^2a_j^2\mid(A+a_j)\cdot A$，

于是 $S_{k+1}=\{A,A+a_1,A+a_2,\cdots,A+a_k\}$满足题设要求.

所以,$n=k+1$ 时命题成立.

从而,对 $n\geqslant2,n\in\mathbf{N}$,命题成立.

例 19 (1981 年英国数学奥林匹克题)证明对任意 $m,n\in\mathbf{N}$,

$$S_{m,n}=1+\sum_{k=1}^{m}(-1)^k\frac{(n+k+1)!}{n!\,(n+k)}$$

都能被 $m!$ 整除,但对某些自然数 m,n,$S_{m,n}$不能被 $m!\,(n+1)$整除.

证明 对 m 用数学归纳法证明

$$S_{m,n}=(-1)^m\frac{(n+m)!}{n!}.\qquad①$$

(1)当 $m=1$ 时,

$$S_{1,n}=1-\frac{(n+2)!}{n!\,(n+1)}=1-(n+2)=-\frac{(n+1)!}{n!},$$

即 $m=1$ 时,①式成立.

(2) 假设对 m,①式成立,那么对 $m+1$,

$$\begin{aligned}S_{m+1,n}&=S_{m,n}+(-1)^{m+1}\frac{(n+m+2)!}{n!(n+m+1)}\\&=(-1)^m\frac{(n+m)!}{n!}+(-1)^{m+1}\frac{(n+m)!\,(n+m+2)}{n!}\\&=(-1)^{m+1}\frac{(n+m)!}{n!}[(n+m+2)-1]\\&=(-1)^{m+1}\frac{(n+m+1)!}{n!},\end{aligned}$$

所以对 $m+1$,①式成立.

因此对所有 $m\in\mathbf{N}$,①式成立.

由于 C_{n+m}^{m}是自然数,则

$$S_{m,n}=(-1)^m\frac{(n+m)!}{n!\,m!}\cdot m!=(-1)^mC_{n+m}^{m}\cdot m!.$$

因而 $S_{m,n}$能被 $m!$ 整除.

当 $n=2$,$m=3$ 时,

$$S_{m,n}=S_{3,2}=-60$$

能被 $m!=3!=6$ 整除,但不能被 $m!\,(n+1)=3!(2+1)=18$ 整除.

例 20 (1995 年第 21 届全俄数学奥林匹克题)试证对于任何正整数 $a_1>1$,都存在严格递增的正整数序列 a_1,a_2,a_3,…,使得对任何 $k\geqslant1$,和数 $a_1^2+a_2^2+\cdots+a_k^2$ 都能被和数 $a_1+a_2+\cdots+a_k$ 整除.

证明 对于给定的正整数 $a_1>1$.

由于 $a_1^2+a_2^2=(a_2-a_1)(a_2+a_1)+2a_1^2$,

所以，只要取 a_2，使 $a_2=2a_1^2-a_1$，就有 $a_1+a_2=2a_1^2$，

从而 $a_1+a_2\mid(a_2-a_1)(a_2+a_1)+2a_1^2$,

即 $a_1+a_2\mid a_1^2+a_2^2$.

且满足 $a_2=2a_1^2-a_1>a_1^2>a_1$.

假设已取定 a_1，a_2，…，a_n 满足题目要求，记

$A_i=a_1^2+a_2^2+\cdots+a_i^2$，$B_i=a_1+a_2+\cdots+a_i$，

则对 $i=1$，2，…，n，有 $B_i\mid A_i$.

由于 $A_{n+1}=A_n+a_{n+1}^2=A_n+(a_{n+1}-B_n)(a_{n+1}+B_n)+B_n^2$

$$=(a_{n+1}-B_n)B_{n+1}+A_n+B_n^2,$$

于是，只要取 a_{n+1} 使 $B_n+a_{n+1}=B_{n+1}=A_n+B_n^2$，即取 $a_{n+1}=A_n+B_n^2-B_n$，就有 $B_{n+1}\mid A_{n+1}$.

且由于 $1<a_1<a_2<\cdots<a_n$，则 $a_{n+1}=A_n+B_n^2-B_n>A_n>a_n^2>a_n$.

于是对 $n+1$ 命题也成立.

从而对所有正整数 k，$B_k\mid A_k$ 成立.

例 21 证明大于 $(\sqrt{3}+1)^{2n}$ 的下一个整数能被 2^{n+1} 整除.

证明 我们首先证明，大于 $(\sqrt{3}+1)^{2n}$ 的下一个整数是

$(1+\sqrt{3})^{2n}+(1-\sqrt{3})^{2n}$.

事实上，由二项式定理，对每个正整数 n，都有整数 A_n 和 B_n，使得

$(1+\sqrt{3})^{2n}=A_n+B_n\sqrt{3}$,

$(1-\sqrt{3})^{2n}=A_n-B_n\sqrt{3}$

成立.

从而 $(1+\sqrt{3})^{2n}+(1-\sqrt{3})^{2n}=2A_n$ 是整数.

由于 $|1-\sqrt{3}|<1$，则

$0<(1-\sqrt{3})^{2n}<1$,

于是 $(1+\sqrt{3})^{2n}+(1-\sqrt{3})^{2n}$ 是大于 $(1+\sqrt{3})^{2n}$ 的下一个整数.

于是问题变为证明 $2A_n$ 能被 2^{n+1} 整除，即变为证明 A_n 能被 2^n 整除.

下面用数学归纳法证明，对所有的正整数 n，A_n 和 B_n 都能被 2^n 整除.

当 $n=1$ 时，$(1+\sqrt{3})^2=4+2\sqrt{3}$，即 $A_1=4$，$B_1=2$ 能被 2^1 整除.

假设命题对 $n=k$ 时成立，即

$2^k | A_k$，$2^k | B_k$.

$$A_{k+1}+B_{k+1}\sqrt{3}=(1+\sqrt{3})^{2(k+1)}=(1+\sqrt{3})^2(1+\sqrt{3})^{2k}$$
$$=(4+2\sqrt{3})(A_k+B_k\sqrt{3})=(4A_k+6B_k)+(2A_k+4B_k)\sqrt{3}.$$

所以 $A_{k+1}=4A_k+6B_k$，$B_{k+1}=2A_k+4B_k$.

于是 $2^{k+1} | A_{k+1}$，$2^{k+1} | B_{k+1}$.

从而命题对 $n=k+1$ 成立.

由以上，均有 $2^n | A_n$，$2^n | B_n$，$n\in\mathbf{N}$.

从而 $2^{n+1} | 2A_n=(1+\sqrt{3})^{2n}+(1-\sqrt{3})^{2n}$.

5. 注意递推法的运用

例 22 （1987 年苏州市高中数学竞赛题）求证 n 是正整数时，大于$(3+\sqrt{5})^{2n}$的最小整数能被 2^{n+1} 整除.

证明 设 $u=3+\sqrt{5}$，$v=3-\sqrt{5}$，则 u，v 是二次方程 $x^2-6x+4=0$ 的两个根.

令 $T_n=u^n+v^n$，

由 $u^2=6u-4$，$v^2=6v-4$，可得

$u^n=6u^{n-1}-4u^{n-2}$，

$v^n=6v^{n-1}-4v^{n-2}$，

于是 $T_n=6T_{n-1}-4T_{n-2}$，$n=2, 3, \cdots$，

从而 T_n 是整数.

由于 $0<3-\sqrt{5}<1$，则

$0<(3-\sqrt{5})^n<1$，

于是 $T_n=(3+\sqrt{5})^n+(3-\sqrt{5})^n$ 是大于$(3+\sqrt{5})^n$ 的最小整数.

由此，命题转化为证明 $2^{n+1} | T_{2n}$.

$$T_{2n}=(3+\sqrt{5})^{2n}+(3-\sqrt{5})^{2n}$$
$$=(14+6\sqrt{5})^n+(14-6\sqrt{5})^n$$
$$=2^n[(7+3\sqrt{5})^n+(7-3\sqrt{5})^n],$$

于是 $2^n | T_{2n}$.

$$T_{2n+1}=(3+\sqrt{5})^{2n+1}+(3-\sqrt{5})^{2n+1}$$
$$=2^n[(3+\sqrt{5})(7+3\sqrt{5})^n+(3-\sqrt{5})(7-3\sqrt{5})^n],$$

所以 $2^n | T_{2n+1}$. ①

下面用数学归纳法证明 $2^{n+1} | T_{2n}$.

当 $n=0$ 时，

$T_0=2$，$2^{0+1}=2$，

所以 $2^{0+1} \mid T_{2\cdot 0}$.

即 $n=0$ 时，$2^{n+1} \mid T_{2n}$ 成立.

假设 $n=k$ 时，有 $2^{k+1} \mid T_{2k}$，那么 $n=k+1$ 时，

$$\begin{aligned}T_{2(k+1)}&=6T_{2k+1}-4T_{2k}\\&=6(6T_{2k}-4T_{2k-1})-4T_{2k}\\&=32T_{2k}-24T_{2k-1}.\end{aligned}$$

由①，$2^{k-1} \mid T_{2k-1}$ 及 $2^{k+1} \mid T_{2k}$，

从而 $2^{k+2} \mid 24T_{2k-1}$，$2^{k+2} \mid 32T_{2k}$，

即 $2^{k+2} \mid T_{2(k+1)}$.

从而对 $n=k+1$，$2^{n+1} \mid T_{2n}$ 成立.

本题得证.

【模拟实战】

1. (1) x,y 均为整数，若 $5 \mid (x+9y)$，求证 $5 \mid (8x+7y)$.

   (2) x,y,z 均为整数，若 $11 \mid (7x+2y-5z)$，求证 $11 \mid (3x-7y+12z)$.

2. （1989 年第 15 届全俄数学奥林匹克题）证明和数 $1\cdot 2\cdot 3\cdot \cdots \cdot 2000\cdot 2001+2002\cdot 2003\cdot \cdots \cdot 4001\cdot 4002$ 能被 4003 整除.

3. （1988 年加拿大数学奥林匹克训练题）证明 $1\cdot 3\cdot 5\cdot \cdots \cdot 1983\cdot 1985+2\cdot 4\cdot 6\cdot \cdots \cdot 1984\cdot 1986$ 能被 1987 整除.

4. （1982 年第 16 届全苏数学奥林匹克题）设 m 和 n 是自然数，证明如果对于某些非负整数 k_1，k_2，…，k_n，数 $2^{k_1}+2^{k_2}+\cdots+2^{k_n}$ 能被 2^m-1 整除，那么 $n\geqslant m$.

5. （1992 年第 55 届莫斯科数学奥林匹克题）在小于 10000 的奇自然数 n 中，是使由 n^9 的后 4 个数码组成的数大于 n 的奇数 n 多，还是使由 n^9 的后 4 个数码组成的数小于 n 的奇数 n 多?

6. （1964 年第 4 届全俄数学奥林匹克题）a，b 及 n 是固定的自然数，且对任何自然数 $k(k\neq b)$，$a-k^n$ 能被 $b-k$ 整除，证明 $a=b^n$.

7. （1989 年列宁格勒数学奥林匹克题）能否找到 100 个互不相同的自然数，使得其中任意 5 个数的乘积都可被这 5 个数的和整除?

8. （1963 年第 24 届美国普特南数学竞赛题）设 x^2-x+a 能整除 $x^{13}+x+90$，试确定正整数 a 的值.

9. （1966 年第 27 届美国普特南数学竞赛题）给定 $mn+1$ 个正整数 a_1，a_2，…，a_{mn+1}，且 $0<a_1<a_2<\cdots<a_{mn+1}$. 证明：存在 $m+1$ 个数，使它们中没有一个数

能够被另一个数整除，或者存在 $n+1$ 个数，使得依小到大顺序排成序列，除最前面的一个数之外，每个数都能被它前面的数整除.

10. （1981 年全国高中数学联赛试题）组装甲、乙、丙三种产品，需用 A、B、C 三种零件. 每件甲需用 A，B 各 2 个；每件乙需用 B，C 各 1 个；每件丙需用 2 个 A 和 1 个 C. 用库存的 A、B、C 三种零件，如组装成 p 件甲产品、q 件乙产品和 r 件丙产品，则剩下 2 个 A 和 1 个 B，但 C 恰好用完. 试证无论怎样改变产品甲、乙、丙的件数，也不能把库存的 A、B、C 三种零件都恰好用完.

11. （IMO－32 预选题）求最大的正整数 k，使得
$$1991^k \mid 1990^{1991^{1992}}+1992^{1991^{1990}}.$$

12. （2004 年捷克和斯洛伐克数学奥林匹克题）求正整数 n，使得 $\frac{n}{1!}+\frac{n}{2!}+\cdots+\frac{n}{n!}$ 是一个整数.

13. （第 45 届越南数学奥林匹克题）已知整数 x，y 满足 $x\neq-1$，$y\neq-1$ 且使得 $\frac{x^4-1}{y+1}+\frac{y^4-1}{x+1}$ 是整数. 求证：$x^4y^{44}-1$ 能被 $x+1$ 整除.

14. （第 17 届日本数学奥林匹克题）n 为十位数字非零的四位数. 若将 n 的前两个数字和后两个数字分别看作两个两位数，求所有满足条件的 n，使得按上述方法拆分后的两个两位数之积是 n 的因数.

15. （2007 年英国数学奥林匹克题）证明：存在无限多个正整数对 (m, n)，使得 $\frac{m+1}{n}+\frac{n+1}{m}$ 为正整数.

16. （2005 年白俄罗斯数学奥林匹克题）设 a，b 是正整数，使得 $79\mid(a+77b)$，且 $77\mid(a+79b)$，求和 $a+b$ 可能存在的最小值.

17. （2007 年波罗的海地区数学竞赛题）设 a、b 是有理数，且 $S=a+b=a^2+b^2$. 证明：S 可以写成一个分式，且分母与 6 互素.

18. （2007 年保加利亚国家数学竞赛题）求所有的正整数 x、y，使得 $(xy^2+2y)\mid(2x^2y+xy^2+8x)$.

19. （第 31 届俄罗斯数学奥林匹克题）证明：对任何整系数多项式 $p(x)$ 和任何正整数 k，存在正整数 n，使得 $p(1)+p(2)+\cdots+p(n)$ 能被 k 整除.

20. （2006 年塞尔维亚和黑山队选拔考试题）求所有自然数 n 和 k $(k>1)$，使得 k 能整除 C_n^1，C_n^2，…，C_n^{n-1} 中的每一个数.

21. （第 54 届白俄罗斯数学奥林匹克题）设正整数 $A=\overline{a_na_{n-1}\cdots a_1a_0}$，$a_n$，$a_{n-1}$，…，$a_0$ 均不为 0，且不全相等（n 为正整数）. 数
$$A_1=\overline{a_{n-1}\cdots a_1a_0a_n},$$

$A_2=\overline{a_{n-2}\cdots a_1a_0a_na_{n-1}}$,

……

$A_k=\overline{a_{n-k}a_{n-k-1}\cdots a_0a_n\cdots a_{n-k+1}}$,

……

$A_n=\overline{a_0a_n\cdots a_1}$

是由 A 循环排列而得. 求 A，使得任意的 $A_k(k=1,2,\cdots,n)$能被 A 整除.

22. (1983 年第 46 届莫斯科数学奥林匹克题) 证明当且仅当 $m-n$ 可被 3^k 整除时，4^m-4^n 可被 3^{k+1}整除. 试对 (1) $k=1$, 2, 3; (2) 任何自然数 k 讨论问题，其中 $m\in\mathbf{N}$, $n\in\mathbf{N}$ 且 $m>n$.

23. (2004 年澳大利亚数学奥林匹克题) 已知非负整数 a、b 和

$Z(a,b)=\frac{(3a)!\ (4b)!}{(a!)^4(b!)^3}$.

证明：(1) 对所有 $a\leqslant b$, $Z(a, b)$ 是一个非负整数；

(2) 对于任何非负整数 b，存在无限多个 a，使得 $Z(a, b)$ 不是整数.

24. (1981 年全国高中数学联赛试题) 证明：对于任何自然数 n 和 k，数 $f(n,k)=2n^{3k}+4n^k+10$ 都不能分解成若干个连续的自然数之积.

第三章 同余

【基础知识】

1. 定义

设 m 为正整数，若整数 a 和 b 被 m 除的余数相同，则称 a 和 b 对模 m 同余，记作 $a\equiv b \pmod m$.

2. 同余的基本性质

(1) $a\equiv a \pmod m$.

(2) $a\equiv b \pmod m \Leftrightarrow m \mid b-a$，即有 $a=b+mq$.

特别地，$a\equiv 0 \pmod m$，即 $m \mid a$.

(3) $a\equiv b \pmod m \Leftrightarrow b=km+a \ (k\in \mathbf{Z})$.

(4) 若 $a\equiv b \pmod m$，则 $b\equiv a \pmod m$.

(5) 若 $a\equiv b \pmod m$，$b\equiv c \pmod m$，则 $a\equiv c \pmod m$.

(6) 若 $a\equiv b \pmod m$，$c\equiv d \pmod m$，则

$a\pm c\equiv b\pm d \pmod m$，

$ac\equiv bd \pmod m$，

$a^n\equiv b^n \pmod m \ (n\in \mathbf{N})$.

(7) 若 $ac\equiv bc \pmod m$，$(c, m)=d$，则

$$a\equiv b\left(\bmod \frac{m}{d}\right),$$

其中符号 (c, m) 表示 c，m 的最大公约数.

特别地，当 $(c, m)=1$ 时，若 $ac\equiv bc \pmod m$，则 $a\equiv b \pmod m$.

(8) 若 $n \mid m$，$a\equiv b \pmod m$，则 $a\equiv b \pmod n$.

(9) 若 d 是 a ，b，m 的公约数，又有 $a\equiv b \pmod m$，则

$$\frac{a}{d}\equiv\frac{b}{d}\left(\bmod \frac{m}{d}\right).$$

(10) 若 $a\equiv b \pmod m$，则 $(a, m)=(b, m)$.

(11) 若 $(a, m)=1$，则必存在 $\bar{a}$，使 $a\bar{a}\equiv 1 \pmod m$.

事实上，取 $\bar{a}$，y，使 $aa+my-1$ 即得.

若 $a|b$，$(a,m)=1$，则 $a\cdot\frac{b}{a}\equiv b(\mathrm{mod}\ m)$，两端乘以 $\bar{a}$，则有

$$\bar{a}b\equiv\bar{a}a\cdot\frac{b}{a}\equiv\frac{b}{a}(\mathrm{mod}\ m).$$

由上可把 $\bar{a}$ 看成 a 的"倒数"．当然，在通常意义下非零的数才有倒数，而在同余的意义下，与模互素的数才有倒数．

3．同余类

由关于模 m 同余的数组成的集合，每一个集合叫做关于模 m 的同余类（或叫做关于模 m 的剩余类）．

由于任何整数被 m 除的余数只能是 0，1，2，…，$m-1$ 这 m 种情形，所以整数集可以按对模 m 同余的关系分成 m 个子集：

A_0，A_1，A_2，…，A_{m-1}．

其中 $A_i=\{qm+i\mid m$ 为模，$q\in\mathbf{Z}$，$0\leqslant i\leqslant m\}$，$i=0$，1，2，…，$m-1$．

所有的 A_i（$i=0$，1，2，…，$m-1$）满足

$$\bigcup_{i=0}^{m-1}A_i=\mathbf{Z},\ \bigcap_{i=0}^{m-1}A_i=\varnothing.$$

4．完全剩余系

从模 m 的 m 个同余类 A_0，A_1，A_2，…，A_{m-1} 中，每一类 A_i 取一数 a_i，则 a_0，a_1，a_2，…，a_{m-1} 叫做模 m 的一个完全剩余系（简称 m 的完系）．显然，完系中的 m 个数分别属于 m 个不同的剩余类．

最简单的模 m 的完全剩余系是 0，1，2，…，$m-1$，也叫做模 m 的最小非负完系．

显然 m 个相继整数构成模 m 的一个完系．

如果 $(a,m)=1$，$a_0,a_1,a_2,\cdots,a_{m-1}$ 是模 m 的一个完系，则 $aa_0+b,aa_1+b,\cdots,aa_{m-1}+b$ 也是模 m 的一个完系．

事实上，只要证明 $aa_0+b,aa_1+b,\cdots,aa_{m-1}+b$ 对模 m 两两不同余．若 $aa_i+b\equiv aa_j+b(\mathrm{mod}\ m)$，因 $(a,m)=1$，则 $a_i\equiv a_j(\mathrm{mod}\ m)$．又 a_0，a_1，…，a_{m-1} 是完系，所以只有 $i=j$．

【典型例题与基本方法】

例 1 证明当且仅当指数 n 不能被 4 整除时，$1^n+2^n+3^n+4^n$ 能被 5 整除，其中 n 是正整数．

证明 不难验证 $1^4=1\equiv1\ (\mathrm{mod}\ 5)$，

$2^4=16\equiv1\ (\mathrm{mod}\ 5)$，

$3^4=81\equiv1 \pmod 5$，

$4^4=256\equiv1 \pmod 5$.

假设 $n=4k+r$，$r=0$，1，2，3.

由以上 $a^4\equiv1 \pmod 5$， $a=1$，2，3，4.

则 $a^{4k}\equiv1 \pmod 5$，

$a^n=a^{4k+r}\equiv a^r \pmod 5$.

由此可得

$S_n=1^n+2^n+3^n+4^n\equiv1^r+2^r+3^r+4^r \pmod 5$.

当 $r=0$，1，2，3，依次有

当 $r=0$ 时，$S_n\equiv4\equiv4 \pmod 5$，

当 $r=1$ 时，$S_n\equiv10\equiv0 \pmod 5$，

当 $r=2$ 时，$S_n\equiv30\equiv0 \pmod 5$，

当 $r=3$ 时，$S_n\equiv100\equiv0 \pmod 5$.

因此，当且仅当 n 不能被 4 整除时，S_n 能被 5 整除.

例 2 假设 a，b，c，d 和 m 是这样的整数，使 am^3+bm^2+cm+d 能被 5 整除，且数 d 不能被 5 整除. 证明：总可以找到这样的整数 n，使得 dn^3+cn^2+bn+a 也能被 5 整除.

证明 首先证明 m 不可能被 5 整除.

事实上，如果 m 能被 5 整除，那么由 $5\mid am^3+bm^2+cm+d$ 可得

$5\mid d$，与题设 $5\nmid d$ 矛盾.

于是 m 只能写成 $m=5k+r$，$r=1$，2，3，4 的形式.

注意到 $1\cdot1\equiv1 \pmod 5$，

$2\cdot3\equiv1 \pmod 5$，

$4\cdot4\equiv1 \pmod 5$.

于是当 m 取 $5k+1$，$5k+2$，$5k+3$，$5k+4$ 时，相应的 n 取 $5t+1$，$5t+3$，$5t+2$，$5t+4$，则必有

$mn\equiv1 \pmod 5$，

$5\mid mn-1$.

设 $A=am^3+bm^2+cm+d$，

$B=dn^3+cn^2+bn+a$.

从 A，B 中消去 d，得

$An^3-B=(mn-1)[a(m^2n^2+mn+1)+bm(mn+1)+cn^2]$，

于是 $5\mid An^3-B$.

再由　$5\mid A$,

可得　$5\mid B-dn^3+cn^2+bn+a$.

例 3　试证对每一个正整数都存在一个它的倍数，该数包含全部 10 个阿拉伯数字.

证法 1　设 $p=1234567890\cdot10^k$，n 为给定的正整数，k 是使 $10^k>n$ 的一个整数，则

$p+1$，$p+2$，…，$p+n$ 是 n 个以 1234567890 开始的十进制数，这 n 个数中必有一个是 n 的倍数.

证法 2　设 n 是给定的正整数，

又设　$A=\overline{1234567890}$,

并记　$\underbrace{AA\cdots A}_{i\text{个}}=\underbrace{12345678901234567890\cdots1234567890}_{i\text{组}}$,

则在数列

$A,\ AA,\ \cdots,\ \underbrace{AA\cdots A}_{n+1\text{组}}$

中，必有两数对 n 同余.

设 $\underbrace{AA\cdots A}_{i\text{组}}$，$\underbrace{AA\cdots A}_{j\text{组}}$ 对 n 同余，则

$\underbrace{AA\cdots A}_{i\text{组}}-\underbrace{AA\cdots A}_{j\text{组}}$

是 n 的倍数，而这个数由全部 10 个阿拉伯数字组成.

例 4　按公元纪年，(1) 年数不能被 4 整除是平年；(2) 年数能被 4 整除，但不能被 100 整除是闰年；(3) 年数能被 100 整除，但不能被 400 整除是平年；(4) 年数能被 400 整除是闰年；(5) 闰年 366 天，平年 365 天. 证明圣诞节在星期三的概率不是 $\frac{1}{7}$.

证明　任何接连 400 个阳历年中，有 303 个平年，97 个闰年，共有

$365\cdot400+97$ (天).

由于　$365\equiv1\pmod 7$,

　　　$400\equiv1\pmod 7$,

　　　$97\equiv-1\pmod 7$,

则　$7\mid365\cdot400+97$.

在 400 年内共有整数个星期，即 20871 个星期.

因此，圣诞节在星期中轮流出现的日子是 400 次.

如果 N 年的圣诞节是在星期三，则圣诞节在星期三的概率是 $\frac{N}{400}$，但

$\frac{N}{400}\neq\frac{1}{7}$.

例5 （1980年第6届全俄数学奥林匹克题）证明在2^1-1，2^2-1，2^3-1，…，$2^{n-1}-1$中至少有一个数能被n整除，其中n为大于1的奇数.

证明 考察数

2^0，2^1，2^2，…，2^{n-1}.

它们被n除的余数设为

r_0，r_1，r_2，…，r_{n-1}.

因为n为大于1的奇数，所以$n\nmid 2^i(i=0,1,\cdots,n-1)$.

所以，r_0，r_1，r_2，…，r_{n-1}这n个余数只有1，2，…，$n-1$这$n-1$种情形，因而有两个余数相等，不妨设为

$r_k=r_l$，$0\leqslant k<l\leqslant n-1$.

于是 $n|2^l-2^k$，

即 $n|2^k(2^{l-k}-1)$.

因为奇数n与偶数2^k互素，则

$n\mid 2^{l-k}-1$.

由于$0<l-k\leqslant n-1$，则$2^{l-k}-1$是2^1-1，2^2-1，…，$2^{n-1}-1$中的一个，于是问题得证.

例6 （1989年列宁格勒数学奥林匹克题）将所有可能的由7个数码所构成的序列（即由0000000到9999999）按某种顺序一个接一个地写出来，证明所得到的70000000位数可被239整除.

证明 显然有

$10^7\equiv 1(\bmod 239)$.

设A和B是两个七位数，则

$\overline{AB}=A\cdot 10^7+B\equiv A+B(\bmod 239)$.

于是所得到的70000000位数与这10000000个7位数之和对模239同余.

这10000000个7位数之和为

$1+2+3+\cdots+9999999=\frac{1}{2}\cdot 10^7(10^7-1)$.

由于$239|10^7-1$，则

所得到的70000000位数能被239整除.

例7 （2006年土耳其国家队选拔赛题）已知整数列$\{x_n\}$满足

$x_{n+1}=x_1^2+x_2^2+\cdots+x_n^2$，$n\geqslant 1$.

求x_1的最小值，使得2006整除x_{2006}.

解 注意到

$$x_{n+1}=\sum_{i=1}^{n}x_i^2=x_n+x_n^2=x_n(x_n+1).$$

所以，$2\mid x_{n+1}$.

故 $2006\mid x_{2006}\Leftrightarrow 1003\mid x_{2006}\Leftrightarrow 17\mid x_{2006}$ 且 $59\mid x_{2006}$.

若 $x_n\equiv c\pmod{17}$，则

$x_n(x_n+1)\equiv 0\pmod{17}\Leftrightarrow c\equiv 0\pmod{17}$ 或 $c\equiv -1\pmod{17}$.

而 $x(x+1)\equiv -1\pmod{17}$ 无解，于是

若 $17\mid x_{2006}$，则

$x_{2006}\equiv x_{2005}(x_{2005}+1)\pmod{17}$.

若 $x_{2005}\equiv -1\pmod{17}$，则 x_{2004} 无解.

所以，$17\mid x_{2005}$.

同上递推知 $17\mid x_2$，从而

$x_1\equiv 0\pmod{17}$ 或 $x_1\equiv -1\pmod{17}$.

若 $x_n\equiv c\pmod{59}$，则

$x_n(x_n+1)\equiv 0\pmod{59}\Leftrightarrow c\equiv 0\pmod{59}$ 或 $c\equiv -1\pmod{59}$.

而 $(x+1)x\equiv -1\pmod{59}$ 无解，故同上可知

$x_1\equiv 0$ 或 $-1\pmod{59}$.

若 $x_1\equiv 0\pmod{59}$，$x_1\equiv 0\pmod{17}$，从而，x_1 最小值为 1003；

若 $x_1\equiv -1\pmod{59}$，$x_1\equiv 0\pmod{17}$，从而，x_1 最小值为 $15\times 59-1=884$；

若 $x_1\equiv -1\pmod{17}$，$x_1\equiv 0\pmod{59}$，从而，x_1 最小值为 118；

若 $x_1\equiv -1\pmod{17}$，$x_1\equiv -1\pmod{59}$，从而，x_1 最小值为 1002.

所以，x_1 最小值为 118.

例 8 （2005 年国家队集训测试题）设 p 是给定的素数，a_1，…，a_k 是 $k(k\geqslant 3)$ 个整数，均不被 p 整除且模 p 互不同余. 记

$$S=\{n\mid 1\leqslant n\leqslant p-1,(na_1)_p<\cdots<(na_k)_p\},$$

这里 $(b)_p$ 表示整数 b 被 p 除的余数. 证明：$|S|<\frac{2p}{k+1}$.

证明 需要一个引理.

引理 记 $b_0=p-a_k$，$b_i=a_i-a_{i-1}$，$i=1, 2, \cdots, k$，这里 $a_0=0$. 令

$S'=\{n\mid 1\leqslant n\leqslant p-1,(b_0n)_p+\cdots+(b_kn)_p=p\}$，则

$|S|=|S'|$.

引理的证明：设有一个 $n\in S$，则有

$0<(a_{i-1}n)_p<(a_in)_p<p, i=2,\cdots,k.$

从而 $0<(a_in)_p-(a_{i-1}n)_p<p$，且

$(a_in)_p-(a_{i-1}n)_p\equiv(b_in)_p\pmod p$，

（由 b_i 定义及带余除法即知）故

$(a_in)_p-(a_{i-1}n)_p=(b_in)_p, i=2,\cdots,k$，

累加得 $(a_kn)_p=(b_1n)_p+\cdots+(b_kn)_p$，

即有[注意 $(b_0n)_p+(a_kn)_p=p$]

$(b_0n)_p+\cdots+(b_kn)_p=p$，

故 $n\in S'$.

反过来，若 $n\in S'$，因 $b_1+\cdots+b_i=a_i(i=1,\cdots,k)$，故

$(a_in)_p\equiv(b_1n)_p+\cdots+(b_in)_p\pmod p$.

因 $0<(a_in)_p<p$ 及 $0<(b_1n)_p+\cdots+(b_in)_p<p$（由 $n\in S'$），从而

$(a_in)_p=(b_1n)_p+\cdots+(b_in)_p(i=1,\cdots,k)$.

于是 $(a_in)_p=(a_{i-1}n)_p+(b_in)_p>(a_{i-1}n)_p, i=1,\cdots,k$，即 $n\in S$，故 $|S|=|S'|$.

现在解决原题. 因 $p\nmid b_i$，故对 $n=1, 2, \cdots, p-1$，$(b_in)_p$ 互不相同，所以对 $i=0, 1, \cdots, k$，有

$$\sum_{n\in S'}(b_in)_p\geqslant 1+2+\cdots+|S'|=\frac{|S'|(|S'|+1)}{2}.$$

将上式对 i 求和，注意 S' 的定义及 $|S|=|S'|$（由引理），得到

$$p|S|=p|S'|=\sum_{n\in S'}((b_1n)_p+\cdots+(b_kn)_p)$$

$$=\sum_{i=1}^{k}\sum_{n\in S'}(b_in)_p\geqslant(k+1)\frac{|S|(|S|+1)}{2}.$$

所以 $|S|<\frac{2p}{k+1}$.

【解题思维策略分析】

1. 灵活运用同余的性质解题

例 9 （1970 年第 4 届全苏数学奥林匹克题）在每张卡片上各写着从 11111 到 99999 的五位数，然后把这些卡片按任意顺序排成一排. 证明所得到的 444445 位数不可能是 2 的幂.

证明 注意到 10^5 除以 11111 时，有余数 1，即

$10^5\equiv1\pmod{11111}$.

记五位数 11111，11112，…，99998，99999 的任意一个排列为

$a_1, a_2, \cdots, a_{88889}$.

把这 88889 个五位数排成一个 444445 位数 A，则

$A=a_1\cdot 10^{444440}+a_2\cdot 10^{444435}+\cdots+a_{88888}\cdot 10^5+a_{88889}$.

由 $10^5\equiv 1 \pmod{11111}$，得

$10^{5k}\equiv 1 \pmod{11111}, k\in \mathbf{N}$.

于是有

$A\equiv a_1+a_2+\cdots+a_{88889} \pmod{11111}$.

由于 $a_1+a_2+\cdots+a_{88889}$

$=11111+11112+\cdots+99999$

$=\frac{11111+99999}{2}\cdot 88889$

$=11111\cdot 5\cdot 88889$,

所以 $A\equiv a_1+a_2+\cdots+a_{88889}\equiv 0 \pmod{11111}$.

于是数 A 能被 11111 整除，因而不可能是 2 的幂.

例 10 （1980 年第 14 届全苏数学奥林匹克题）接连写出 19 至 80 的两位数，问：所得到的数 19202122…787980 能被 1980 整除吗?

解 设 $A=19202122\cdots 7980$.

显然 $20\mid A$.

由于 $100^k=(99+1)^k=99M+1$，其中 M 为正整数，k 为正整数，

所以 $100^k\equiv 1 \pmod{99}$.

于是有

$A=19\cdot 100^{61}+20\cdot 100^{60}+\cdots+79\cdot 100+80$

$\equiv(19+20+21+\cdots+79+80)$

$\equiv 31\cdot 99$

$\equiv 0 \pmod{99}$,

从而 $99\mid A$.

又因为 $(20,99)=1$，所以

$20\cdot 99=1980\mid A$.

例 11 试求 $10^{10}+10^{10^2}+10^{10^3}+\cdots+10^{10^{10}}$ 被 7 除的余数.

解 设 $A=10^{10}+10^{10^2}+10^{10^3}+\cdots+10^{10^{10}}$.

首先我们证明，若 $6\mid n-r$，则 $7\mid 10^n-10^r, (n>r)$.

事实上，

$10^n-10^r=10^r(10^{n-r}-1)=10^r(10^{6k}-1)=((10^6)^k-1)\cdot 10^r$.

因为 $10^6\equiv 1 \pmod 7)$，所以

$(10^6)^k-1\equiv 0 \pmod 7$,

即 $7|10^n-10^r$.

另一方面，$6|10^k-10(k\geqslant1)$，则

$A-10\cdot10^{10}+10\cdot10^{10}$

$=(10^{10}-10^{10})+(10^{10^2}-10^{10})+\cdots+(10^{10^{10}}-10^{10})+10\cdot10^{10}$.

由于 $6|10^k-10$，则

$7|10^{10^k}-10^{10}$.

于是有

$A\equiv10\cdot10^{10}$

$\quad=10^{11}$

$\quad=(7+3)^{11}$

$\quad\equiv3^{11}$

$\quad\equiv3^5\cdot3^6 \pmod 7$.

由于 $3^5\equiv5 \pmod 7$，

$\quad 3^6\equiv1 \pmod 7$，

于是 $A\equiv5 \pmod 7$.

即 A 被 7 除的余数是 5.

例 12 （*1977 年第 38 届美国普特南数学竞赛题*）证明 $C_{pa}^{pb}\equiv C_a^b \pmod p$ 对所有整数 p，a 和 b 都成立，这里 p 为素数，$a\geqslant b\geqslant0$.

证明 可以证明 $C_p^i\equiv0 \pmod p$ 对素数 p 及 $i=1,2,\cdots,p-1$ 成立.

从而对整数 x，

$(1+x)^p\equiv1+x^p \pmod p$.

$$\sum_{k=0}^{pa}C_{pa}^kx^k=(1+x)^{pa}$$
$$=[(1+x)^p]^a$$
$$\equiv(1+x^p)^a$$
$$\equiv\sum_{j=0}^{a}C_a^jx^{jp} \pmod p.$$

因为在等式

$$\sum_{k=0}^{pa}C_{pa}^kx^k\equiv\sum_{j=0}^{a}C_a^jx^{jp} \pmod p$$

中同次幂的系数必对于模 p 同余，所以在 $k=pb$ 及 $j=b$ 时，有

$C_{pa}^{pb}=C_a^b \pmod p$.

例 13 （*2005 年克罗地亚数学奥林匹克题*）已知 99 个小于 100 且可以相等的正整数．若所有 2 个、3 个或更多个数的和都不能被 100 整除，证明：所有的数均相等.

证明 记给定的数为 $n_1, n_2, \cdots, n_{99}$.

假设结论不成立，即有两个不同的数，例如 $n_1 \neq n_2$.

考察以下 100 个数：

$S_1 = n_1$，$S_2 = n_2$，$S_3 = n_1 + n_2$，$\cdots$，$S_{100} = n_1 + n_2 + \cdots + n_{99}$.

由假设，数 $S_i(i=1,2,\cdots,100)$ 不能被 100 整除. 由抽屉原理，这些数中至少有两个被 100 除的余数相同，将它们记为 S_k，S_l，且 $k>l$. 显然，

$\{S_k, S_l\} \neq \{S_1, S_2\}$.

因为 S_k 和 S_l 被 100 除的余数相同，于是，$S_k - S_l$ 能被 100 整除，即

$100 | [(n_1 + n_2 + \cdots + n_k) - (n_1 + n_2 + \cdots + n_l)]$.

所以，$100 | (n_{l+1} + n_{l+2} + \cdots + n_k)$，与假设矛盾.

因此，所有的数均相等.

例 14 （2007 年捷克-斯洛伐克-波兰数学竞赛题）已知 $a_1 = a_2 = 1$，$a_{k+2} = a_{k+1} + a_k (k \in \mathbf{N}_+)$. 证明：对任意正整数 m，必存在一个 k，满足 $m | (a_k^4 - a_k - 2)$.

证明 若 $m=1$，则结论显然成立.

当 $m \geqslant 2$ 时，设 $a_i \equiv b_i \pmod m (0 \leqslant b_i < m)$，则

$b_i \equiv b_{i-1} + b_{i-2} \pmod m$.

由上式可以看出，数对 (b_i, b_{i+1}) 决定了前后项，且不能取 $(0,0)$. 这是因为若 $(b_i, b_{i+1}) = (0,0)$，则由递推公式知整个数列模 m 为 0，与 $a_1 = 1$ 矛盾.

故 (b_i, b_{i+1}) 的可能取值为 $m^2 - 1$ 个.

由抽屉原理知，必存在 $1 \leqslant i < j \leqslant m^2$，使得

$(b_i, b_{i+1}) = (b_j, b_{j+1})$.

由上式知 $b_i = b_j$，$b_{i+1} = b_{j+1}$.

令 $p = j - i$，则 $b_{k+p} = b_k$，即

$a_{k+p} \equiv a_k \pmod m$.

因为 $a_1 \equiv a_2 \equiv 1 \pmod m$，所以，

$a_{p+1} \equiv a_{p+2} \equiv 1 \pmod m$.

因此，$a_p \equiv 0 \pmod m$，

$a_{p-1} \equiv 1 \pmod m$，

$a_{p-2} \equiv -1 \pmod m$，

$a_{tp-2} \equiv -1 \pmod m$，

其中，$t \in \mathbf{N}_+$，使得 $tp - 2 > 0$.

取 $k = tp - 2$，则有

$a_k^4 - a_k - 2 \equiv 0 \pmod m$.

例 15 （CMO-8试题）设 n 是奇数．试证存在 $2n$ 个整数 a_1，a_2，…，a_n；b_1，b_2，…，b_n，使得对任意一个整数 $k(0<k<n)$，下列 $3n$ 个数 a_i+a_{i+1}，a_i+b_i，$b_i+b_{i+k}(i=1, 2, \cdots, n)$；其中 $a_{n+1}=a_1$，$b_{n+j}=b_j$，$0<j<n$）被 $3n$ 除所得的余数互不相同．

证明 设 $a_i=3i-2$，$b_i=3i-3(i=1, 2, \cdots, n)$，则有

$$a_i+a_{i+1}=3i-2+3(i+1)-2$$
$$=6(i-1)+5\equiv 2 \pmod 3, \quad ①$$
$$a_i+b_i=3i-2+3i-3$$
$$=6(i-1)+1\equiv 1 \pmod 3, \quad ②$$
$$b_i+b_{i+k}=3i-3+3(i+k)-3$$
$$=6(i-1)+3k\equiv 0 \pmod 3. \quad ③$$

由此可见，①，②，③三组数对模 3 不同余，因此对模 $3n$ 也不同余，亦即任何来自不同组的两个数被 $3n$ 除所得的余数不相同．

下证同一组内任何两数对模 $3n$ 不同余．

事实上，若同一组内有两数对模 $3n$ 同余，即存在 p，q，$1\leqslant p<q\leqslant n$，使得

$$6(p-1)+r\equiv 6(q-1)+r \pmod{3n},$$

其中 $r=1$，2 或 $3k$，则

$$6(p-1)\equiv 6(q-1) \pmod{3n},$$
$$6p\equiv 6q \pmod{3n},$$
$$2p\equiv 2q \pmod n,$$
$$2(p-q)\equiv 0 \pmod n.$$

因为 n 是奇数，则 $2\nmid n$，又 $|p-q|<n$，故必有 $2(p-q)=0$．

于是有 $p=q$，与 $p<q$ 矛盾．

所以无论第一组($r=2$)，第二组($r=1$)或第三组($r=2k$)，组内任何两数对模 $3n$ 不同余．

综上所述，所取的 $2n$ 个数 a_1，a_2，…，a_n；b_1，b_2，…，b_n 为符合题目要求的 $2n$ 个整数．

2. 善于利用同余类、完系处理问题

例 16 （1991年澳大利亚数学通讯竞赛题）求具有以下性质的最小正整数 n，使得对于任意选定的 n 个整数，至少存在两个数，它们的和或差能被 1991 整除．

解 取 996 个整数的集合 $M=\{a_i|a_i=0,1,2,\cdots,995\}$，则

对于所有的 $i\neq j$，i，$j=0$，1，2，…，995，

$$a_i+a_j\leqslant 995+994=1989,$$

$0<|a_i-a_j|\leqslant 995$.

所以 M 中任意两数的和与差都不是 1991 的倍数.

设 $n=997$，a_1，a_2，…，a_{997} 是任意给定的 997 个整数.

若 $a_i\not\equiv a_j \pmod{1991}$，对所有 $i\neq j$，则由于

-995，-994，…，0，1，2，…，995

是 1991 的完全剩余类，故不妨假设 $|a_i|\leqslant 995$.

此时，由于 $n=997>996$，所以至少存在两个不同的数 a_i，a_j，使得 $a_i=\quad a_j$，于是有

$1991|(a_i+a_j)$.

例 17 （IMO－30 预选题）连接正 n 边形的顶点，获得一个闭的 n-折线. 证明若 n 为偶数，则在连线中有两条平行线；若 n 为奇数，连线中不可能恰有两条平行线.

证明 依反时针顺序将正 n 边形的顶点标上 0，1，2，…，$n-1$.

因此，闭的 n-折线可以用这 n 个数的一个排列

$a_0=a_n$，a_1，a_2，…，a_{n-1}

来唯一表示.

显然

$$a_ia_{i+1}/\!/a_ja_{j+1}\Leftrightarrow\overset{\frown}{a_{i+1}a_j}=\overset{\frown}{a_{j+1}a_i}$$
$$\Leftrightarrow a_i+a_{i+1}\equiv a_j+a_{j+1}\pmod n.$$

若 n 为偶数，则

$2\nmid n-1$.

所以完全剩余系的和

$$0+1+2+\cdots+(n-1)=\frac{n(n-1)}{2}\not\equiv 0\pmod n.$$

而

$$\begin{aligned}\sum_{i=0}^{n-1}(a_i+a_{i+1})&=\sum_{i=0}^{n-1}a_i+\sum_{i=0}^{n-1}a_{i+1}\\&=2\sum_{i=0}^{n-1}a_i\\&=n(n-1)\\&\equiv 0\pmod n.\end{aligned}\qquad ①$$

所以 a_i+a_{i+1}，$i=0$，1，2，…，$n-1$ 不是关于模 n 的完全剩余系.

于是必有 $i\neq j(0\leqslant i,j\leqslant n-1)$，使

$a_i+a_{i+1}\equiv a_j+a_{j+1}\pmod n$，

因而必有一对边 $a_ia_{i+1}//a_ja_{j+1}$.

若 n 为奇数，并且恰有一对边平行，设

$a_ia_{i+1}//a_ja_{j+1}$.

这时，在 a_0+a_1，a_1+a_2，a_2+a_3，…，$a_{n-1}+a_0$ 中恰有一个剩余类 r 出现两次，因而也恰少了一个剩余类 s.

又由 $2\mid n-1$，则

$$\begin{aligned}\sum_{i=0}^{n-1}(a_i+a_{i+1}) &\equiv 0+1+\cdots+(n-1)+r-s\\ &=\frac{n(n-1)}{2}+r-s\\ &\equiv r-s \pmod n.\end{aligned}$$

再由①式得

$$\sum_{i=1}^{n-1}(a_i+a_{i+1})\equiv 0 \pmod n.$$

从而 $r\equiv s \pmod n$.

导致矛盾.

这表明，若 n 为奇数，不可能恰有一对边平行.

例 18 在小于 10000 的正整数中，有多少个整数 x，可使 2^x-x^2 能被 7 整除?

解 首先我们证明

$$2^{21+r}-(21+r)^2\equiv 2^r-r^2 \pmod 7, \quad ①$$

其中 $r\in\{1,2,3,\cdots,21\}$.

事实上，由 $2^{21}=(2^3)^7=8^7\equiv 1 \pmod 7$，则

$2^{21+r}\equiv 2^r \pmod 7$.

又 $(21+r)^2=21^2+42r+r^2\equiv r^2 \pmod 7$，从而①式成立.

由①式可知，2^x-x^2 被 7 除的余数以 21 为周期呈周期性变化.

令 $x=1$，2，…，21，可求出 2^x-x^2 中有 6 个数能被 7 整除.

即 $x=2$，4，5，6，10，15 时，2^x-x^2 被 7 整除.

由于 $10000=476\cdot 21+4$，

于是从 1 到 10000 中有 $476\cdot 6+1=2857$ 个 x，使 2^x-x^2 能被 7 整除.

例 19 （IMO－44 预选题）设 m 是一个大于 1 的固定整数，数列 x_0，x_1，x_2，…定义如下：

$$x_i=\begin{cases}2^i, & 0\leqslant i\leqslant m-1;\\ \sum_{j=1}^{m}x_{i-j}, & i\geqslant m.\end{cases}$$

求 k 的最大值，使得数列中有连续的 k 项均能被 m 整除.

解 设 r_i 是 x_i 模 m 的余数，在数列中按照连续的 m 项分成块，则余数最多有 m^m 种情况出现. 由抽屉原则，有一种类型的情况会重复出现. 因为定义的递推式可以向后递推，也可以向前递推，所以，数列$\{r_i\}$是周期数列.

由已知条件可得向前的递推公式为

$$x_i=x_{i+m}-\sum_{j=1}^{m-1}x_{i+j}.$$

由其中的 m 项组成的余数分别为 $r_0=1$，$r_1=2$，…，$r_{m-1}=2^{m-1}$，求这 m 项前面的 m 项模 m 的余数，由向前的递推公式可得，前 m 项模 m 的余数分别为 $\underbrace{0,0,\cdots,0}_{m-1项},1$. 结合余数数列的周期性，得 $k\geqslant m-1$.

另一方面，若在余数数列$\{r_i\}$中有连续的 m 项均为 0，则由向前的递推公式和向后的递推公式可得，对于所有的 $i\geqslant 0$，均有 $r_i=0$，矛盾.

所以，k 的最大值为 $m-1$.

例 20 （1989 年国家集训队选拔试题）已知 $v_0=0$，$v_1=1$，$v_{n+1}=8v_n-v_{n-1}$，$n=1,2,\cdots$. 求证在数列$\{v_n\}$中没有形如 $3^\alpha\cdot 5^\beta$(α,β为正整数)的项.

证明 直接计算$\{v_n\}$的前几项：

$v_0=0$，$v_1=1$，$v_2=8$，$v_3=63$，$v_4=496$，$v_5=3905$，$v_6=30744$，…

从中可以发现 $v_3=63$，$v_6=30744$ 都是 3 和 7 的倍数，且其余的项 v_1，v_2，v_4，v_5 都不是 3 或 7 的倍数.

我们猜测：

$$3\mid v_n\Leftrightarrow 7\mid v_n. \qquad ①$$

下面证明这个猜测.

先考虑模 3.

数列$\{v_n\}$被 3 除的余数($n=0,1,2,\cdots$)前几项为

$0,1,-1,0,1,-1,\cdots$

于是有

$v_3\equiv v_0 \pmod 3$，

$v_4\equiv v_1 \pmod 3$.

假设有 $v_{k+3}\equiv v_k \pmod 3$ ($k\leqslant n$).

则由 $v_{n+1}=8v_n-v_{n-1}$，可得

$$\begin{aligned}v_{k+4}&=8v_{k+3}-v_{k+2}\\&\equiv 8v_k-v_{k-1}\\&=v_{k+1}\pmod 3.\end{aligned}$$

因此由数学归纳法证明了

$v_{n+3}\equiv v_n(\bmod 3), n=0,1,2,\cdots$.

即$\{v_n\}$以 3 为模的余数列为以 3 为周期的周期数列，且由它的前三项为 0，1，-1（从 v_0 开始），所以有

$3\mid v_n \Leftrightarrow 3\mid n$. ②

再考虑模 7.

$\{v_n\}$被 7 除的余数列的前几项为

$v_0\equiv 0\ (\bmod 7)$，$v_1\equiv 1\ (\bmod 7)$，$v_2\equiv 1\ (\bmod 7)$，$v_4\equiv 0\ (\bmod 7)$，

$v_5\equiv -1\ (\bmod 7)$，$v_6\equiv -1\ (\bmod 7)$，$v_7\equiv 0\ (\bmod 7)$，$v_8\equiv 1(\bmod 7)$.

仿上可以用数学归纳法证明，$\{v_n\}$以 7 为模的余数列是以 6 为周期的周期数列，且有

$7\mid v_n \Leftrightarrow 3\mid n$. ③

由②③可得①.

由①可知，数列$\{v_n\}$没有形如 $3^\alpha\cdot 5^\beta$ 的项，其中 α，β 为正整数.

3. 同余是一种映射

例 21 （CMO - 12 试题）设 $A=\{1,2,3,\cdots,17\}$. 对于一一映射 $f:A\rightarrow A$，记 $f^{[1]}(x)=f(x)$，$f^{[k+1]}(x)=f(f^{[k]}(x))$，$k\in\mathbf{N}$. 又 f 满足条件：

存在自然数 M，使得：

(1) 当 $m<M$，$1\leqslant i\leqslant 16$ 时，有

$f^{[m]}(i+1)-f^{[m]}(i)\not\equiv\pm 1(\bmod 17)$,

$f^{[m]}(1)-f^{[m]}(17)\not\equiv\pm 1(\bmod 17)$.

(2) 当 $1\leqslant i\leqslant 16$ 时，

$f^{[M]}(i+1)-f^{[M]}(i)\equiv 1$ 或 $-1(\bmod 17)$,

$f^{[M]}(1)-f^{[M]}(17)\equiv 1$ 或 $-1(\bmod 17)$.

试对满足上述条件的一切 f，求所对应的 M 的最大可能值，并证明你的结论.

解 所求的 $M_0=8$，先证 $M_0\geqslant 8$.

事实上，可令映射 $f(i)\equiv 3i-2(\bmod 17)$，其中 $i\in A$，$f(i)\in A$.

若 $f(i)\equiv f(j)(\bmod 17)$，则

$3i-2\equiv 3j-2(\bmod 17)$，即 $i\equiv j(\bmod 17)$.

所以 $i=j$.

因此，映射 f 是从 A 到 A 的一一映射.

又由映射 f 的定义，易知

$f^{[n]}(i)=3^n\cdot i-3^n+1 \pmod{17}$.

若$\begin{cases}f^{[M]}(i+1)-f^{[M]}(i)\equiv 1 \text{ 或 } -1 \pmod{17},\\ f^{[M]}(1)-f^{[M]}(17)\equiv 1 \text{ 或} -1 \pmod{17},\end{cases}$

即$\begin{cases}[3^M(i+1)-3^M+1]-[3^M\cdot i-3^M+1]\equiv 1 \text{ 或} -1 \pmod{17},\\ 1-[3^M\times 17-3^M+1]=1 \text{ 或} -1 \pmod{17},\end{cases}$

即 $3^M\equiv 1$ 或 $-1 \pmod{17}$.

但 $3^1\equiv 3 \pmod{17}$，$3^2=9 \pmod{17}$，$3^3=10 \pmod{17}$，$3^4=13 \pmod{17}$，$3^5=5 \pmod{17}$，$3^6=15 \pmod{17}$，$3^7=11 \pmod{17}$，$3^8\equiv -1 \pmod{17}$，故

$M_0\geqslant 8$.

下面再证 $M_0\leqslant 8$.

任作一个凸 17 边形 $A_1A_2\cdots A_{17}$，记作 G.

我们规定：当 $i=17$ 时，取 $i+1=1$；当 $i=1$ 时，取 $i-1=17$.

然后按如下规则连线段：若 $1\leqslant m<M_0$，当 $f^{[m]}(i)=a, f^{[m]}(i+1)=b$ 时，就连线段 A_aA_b.

显然，所连线段必为 G 的对角线. 下面证明，所连的对角线没有重复.

若有两条对角线连线相同，即存在 i，j 及 $M_0>p>q>0$，使

$f^{[p]}(i)=f^{[q]}(j)$,

$f^{[p]}(i+1)=f^{[q]}(j-1)$,或 $f^{[p]}(i+1)=f^{[q]}(j+1)$.

于是，有 $f^{[p-q]}(i)=j$,

$f^{[p-q]}(i+1)=j+1$,或 $f^{[p-q]}(i+1)=j-1$,

且 $M_0>p-q>0$. 这与 M_0 的定义矛盾.

故所连对角线没有重复.

但 G 共有 17×7 条对角线，所以

$17\times(M_0-1)\leqslant 17\times 7$,即 $M_0\leqslant 8$.

故 $M_0=8$.

例 22 求所有满足 f：$\mathbf{N}_+\to\mathbf{N}_+$ 的函数，存在 $k\in\mathbf{N}_+$ 和一个素数 p，使得对任何 $n\geqslant k$，都有 $f(n+p)=f(n)$. 同时还要满足：若 $m|n$，就有 $f(m+1)$ $(f(n)+1)$.

解 对于 $n\geqslant k$，若 $n\not\equiv 1 \pmod{p}$，即 $(n-1,p)=1$，则存在一个正整数 k_0，使得 $(n-1)|(n+k_0p)$，所以，$f(n)|(f(n+k_0p)+1)$.

又 $f(n)=f(n+k_0p)$，所以，$f(n)|1$.

故对任意 $n\geqslant k, n\not\equiv 1 \pmod{p}$，有 $f(n)=1$.

考虑任意的 $n>1$.

由于 $(n-1)|(n-1)kp$,所以,

$f(n)|(f((n-1)kp)+1)=2$.

故对于任何 $n\neq1$，都有 $f(n)\in\{1,2\}$.

这样就有两种情况.

(1) 对全部 $n\geqslant k$，$n\equiv1(\bmod p)$，有 $f(n)=2$.

考虑 $n<k$，或 $(n-1,p)=1$，则存在一个数 $m\geqslant k$，满足

$(n-1)|m$ 和 $p|(m-1)$.

于是，有 $f(n)|(f(m)+1)=3$.

故 $f(n)=1$.

所以，当 $n<k, n\not\equiv1(\bmod p)$ 时，$f(n)=1$.

此时，满足条件的函数可以定义为：

当 $n\not\equiv1(\bmod p)$ 时，$f(n)=1$；

当 $n\geqslant k, n\equiv1(\bmod p)$ 时，$f(n)=2$；

当 $1<n<k, n\equiv1(\bmod p)$ 时，$f(n)=1$ 或 2；

$f(1)$ 取满足 $f(2)|(f(1)+1)$ 的任意正整数.

(2) 对全部 $n\geqslant k$，$n\equiv1(\bmod p)$，有 $f(n)=1$.

在这种情况中，对于任意 $n\geqslant k$，都有 $f(n)=1$.

令 $S=\{a|f(a)=2, a<k\}$. 由定义知，不存在 m、$n\in S$，使得 $(m-1)|n$.

此时，满足题目条件的函数可以这样定义：

S 是一个正整数的有限子集，不存在 m、$n\in S$，使得 $(m-1)|n$.

对于 $n>1$，有 $f(n)=2$ 的充分必要条件是 $n\in S$，$f(1)$ 可以定义为满足条件 $f(2)|(f(1)+1)$ 的任意正整数.

4. 借助于同余处理问题

例 23 （*第 57 届白俄罗斯数学奥林匹克题*）将 2007 个整数放在一个圆周上，使得任意相邻的五个数中有三个的和等于另两个数的和的两倍. 证明：这 2007 个数都是 0.

证明 设圆周上的 2007 个整数依逆时针排列分别为 x_1，x_2，…，x_{2007}，则相邻的五个数的和为其中两个数的和的 3 倍. 特别地，有

$$\begin{aligned}0&\equiv x_1+x_2+x_3+x_4+x_5\\&\equiv x_2+x_3+x_4+x_5+x_6(\bmod 3).\end{aligned}$$

从而，$x_1\equiv x_6(\bmod 3)$.

同理，对于 $i=1$，2，…，2007，有

$x_i\equiv x_{i+5}(\bmod 3)$，

其中，当 $j\equiv k(\bmod 2007)$ 时，设 $x_j=x_k$.

又 5 和 2007 互素，则对于任意的 i、j($i=1,2,\cdots,2007$, $j=1,2,\cdots,2007$)，有

$x_i\equiv x_j \pmod 3$.

对于任意连续的五个数 a、b、c、d、e，因为 $a\equiv b\equiv c\equiv d\equiv e \pmod 3$，所以，

$0\equiv a+b+c+d+e\equiv 5a \pmod 3$.

于是，$a\equiv 0 \pmod 3$.

从而，对于所有的 i($i=1,2,\cdots,2007$)，

$x_i\equiv 0 \pmod 3$.

设 $y_i=\frac{x_i}{3}$($i=1,2,\cdots,2007$)，则 y_i 也满足条件. 继续这样的过程，每次都能得到 2007 个新的数满足条件，所有数都满足是原来的数除以 3 的任意整数次幂.

因此，所有的数一定都是零.

例 24 (2007 年保加利亚国家数学竞赛题) 甲乙两人玩下面的游戏：甲先将一堆 n 个石子分成三堆，每堆至少一个石子，且有一堆石子的数目大于另外两堆中每一堆石子的数目. 然后，乙用同样的方法分石子数目最多的一堆. 甲乙交换进行，谁分最后一次谁就获胜. 对于形如 $n=a^b$ (正整数 a、$b>1$) 的数，哪些使得乙有获胜策略?

解 当 $n=1$, 2, 3 时，石子无法分.

当 $n=4$, 5, 6, 7 时，甲有获胜策略 (因为甲可以使石子最多的一堆的数目为 2 或 3).

当 $n=8$, 9 时，甲操作一次以后，石子最多的一堆的数目在 4 与 7 之间 (包含 4 与 7)，因此，乙有获胜策略.

类似地，当 $10\leqslant n\leqslant 9+8+8=25$ 时，甲有获胜策略 (因为甲可以使石子最多的一堆的数目为 8 或 9)，等等.

从而，由归纳法知，当且仅当 $n=3^k$ 或 3^k-1($k>1$) 时，乙有获胜策略.

3^k 和 $3^2-1=2^3$ 明显满足条件.

下面证明：不存在其他的形如 a^b 的数能使乙有获胜策略.

假设 $a^b=3^k-1$.

因为 $a^2\equiv 0,1 \pmod 3$，则 b 为奇数，所以，

$(a+1)(a^{b-1}-a^{b-2}+\cdots-a+1)=3^k$.

设 $a+1=3^i$，$a^{b-1}-a^{b-2}+\cdots-a+1=3^{k-i}$，其中，整数 i、k 满足 $0<i<k$.

因 $a^{b-1}-a^{b-2}+\cdots-a+1=A(a+1)+b$，其中，$A$ 为整数，所以，b 可以被 3 整除.

设 $c=a^{\frac{b}{3}}$，则

$3^k=c^3+1=(c+1)[(c+1)^2-3c]$.

设 $c+1=3^j$，$(c+1)^2-3c=3^{k-j}$，其中，整数 j、k 满足 $0<j<k$.

因为 $9|(c+1)^2$，$9\nmid 3c$，所以，$k-j=1$.

于是，$3^{2j}-3(3^j-1)=3$，即 $3^{2j-1}=3^j$.

因此，$j=1$，$k=2$，$c=2$，$a=2$，$b=3$.

例 25 （1988 年前南斯拉夫数学竞赛题）有 27 个国家参加的一次国际会议，每个国家有两名代表．求证：不可能将 54 位代表安排在一张圆桌的周围就坐，使得任一国的两位代表之间都夹有 9 个人.

证明 将 54 个座位按逆时针编号为

1，2，3，…，53，54.

如果满足要求的排法存在，由于任一国的两位代表之间都夹有 9 个人，则不妨设 1 和 11 是同一国的代表，于是

11 和 21 不是同一国的代表，

21 和 31 是同一国的代表，

31 和 41 不是同一国的代表，

41 和 51 是同一国的代表，

51 和 61(=7) 不是同一国的代表，

7 和 17 是同一国的代表，

因以上，$20k+1$ 和 $20k+11$ 是同一国的代表．若 $20k+1$ 与 $20k+11$ 大于 54，则取它们被 54 除的余数为号码的位置.

特别地，$k=13$ 时，261 和 271 是同一国的代表，然而

$261\equiv 45 \pmod{54}$，$271\equiv 1 \pmod{54}$，

则 1 和 45 是同一国的代表，与 1 和 11 是同一国的代表矛盾.

于是，不可能得到任一国的两位代表之间都夹有 9 个人的排法.

【模拟实战】

习题 A

1. 求 $47^{47^{\cdots^{47}}}$ 的个位数字，这里共有 $k(>1)$ 个 47.
2. 已知 $ab\equiv -1 \pmod{24}$，求证：$24|(a+b)$.
3. 求证：$7|(2222^{5555}+5555^{2222})$.
4. 求证：$37|(8888^{2222}+7777^{3333})$.

5. 解同余式　$5x\equiv 11 \pmod{43}$.
6. 解同余式　$111x\equiv 75 \pmod{321}$.
7. 给出一个数能否被 11 整除的判别方法.
8. 已知 $99\mid\overline{141x28y3}$，求 x，y.
9. 证明：$15\nmid(n^2+n+2)$.
10. 证明：当 n 为奇数时，$1947\mid(46^n+296\cdot 13^n)$.
11. 对任给的 97 个互异的正整数 a_1，a_2，…，a_{97}，试证其中一定存在四个正整数，仅用减号、乘号和括号将它们适当组合为一个算式，其结果是 1984 的倍数.
12. 已知存在正整数 n，能使数$\underbrace{11\cdots11}_{n个}$被 1987 整除，求证数

$$p=\underbrace{11\cdots11}_{n个}\underbrace{99\cdots99}_{n个}\underbrace{88\cdots88}_{n个}\underbrace{77\cdots77}_{n个}和$$

$$q=\underbrace{11\cdots11}_{n+1个}\underbrace{99\cdots99}_{n+1个}\underbrace{88\cdots88}_{n+1个}\underbrace{77\cdots77}_{n+1个}$$

都能被 1987 整除.

13. 证明对于任何整数 $k\geqslant 0$，$2^{6k+1}+3^{6k+1}+5^{6k}+1$ 能被 7 整除.
14. $1971^{26}+1972^{27}+1973^{28}$能被 3 整除吗?
15. (2004 年德国数学竞赛题) 有一个游戏，开始在黑板上写上 1，2，…，2004. 游戏的每一步包含下列步骤：
    (1) 在黑板上任意选择一些数构成的集合；
    (2) 将这些数之和模 11 的余数写在黑板上；
    (3) 擦掉先前选的这些数.
    当游戏进行到黑板上只留下两个数时，一个是 1000，问另一个数是多少?
16. (2007 年克罗地亚数学奥林匹克题) 证明：对任意正整数 a、b、c、d，整数 $(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$被 12 整除.
17. (1987 年第 21 届全苏数学奥林匹克题) 证明对每个自然数 n，$1^{1987}+2^{1987}+\cdots+n^{1987}$不能被 $n+2$ 整除.
18. (1990 年日本数学奥林匹克代表队选拔试题) 某正整数的平方，其末三位是非零的相同数字，求具有该性质的最小正整数.
19. (1976 年美国纽约数学奥林匹克题) 设 a，a_0，a_1，…，a_n 是任意整数，试问：整数 $\sum\limits_{k=0}^{n}(a^2+1)^{3k}a_k$ 被 a^2+a+1(或被 a^2-a+1) 整除的必要且充分条件是整数 $\sum\limits_{k=0}^{n}(-1)^k a_k$ 被 a^2+a+1(或被 a^2-a+1) 整除. 对否?
20. (1990 年浙江省高中数学夏令营试题) 设正整数 k，使集合 $X=\{3^{31},3^{31}+1,\cdots,$

$3^{31}+k\}$可以分解为三个不相交的子集 A、B 和 C 的并集，且这三个集的元素之和等于同一个值.

求证 $k\neq 1 \pmod 3$，试找出一列具有这样性质的 k.

21. （1987 年第 2 届中国东北三省数学邀请赛试题）有 1987 片玻璃片，每片上涂有红、黄、蓝三色之一. 进行下列操作：将不同颜色的两块玻璃片擦净，然后涂上第三种颜色（例如将一块蓝玻璃和红玻璃片上的红色与蓝色擦掉，然后在两片上涂上黄色）. 证明：

(1) 无论开始时，红、黄、蓝玻璃片各有多少片，总可以经过有限次操作而使所有玻璃片涂有同一种颜色；

(2) 最后变成哪一种颜色，与操作顺序无关.

22. （2006 年国家队集训测试题）设 a_i，$b_i(i=1,2,\cdots,n)$是有理数，使得对任意的实数 x 都有 $x^2+x+4=\sum_{i=1}^{n}(a_ix+b_i)^2$. 求 n 的最小可能值.

习题 B

1. （IMO-28 预选题）设 x_1，x_2，$\cdots$，x_n 为 n 个整数，k 为小于 n 的整数，令

$S_1=x_1+x_2+\cdots+x_k$，$T_1=x_{k+1}+x_{k+2}+\cdots+x_n$，

$S_2=x_2+x_3+\cdots+x_{k+1}$，$T_2=x_{k+2}+x_{k+3}+\cdots+x_n+x_1$，

$S_3=x_3+x_4+\cdots+x_{k+2}$，$T_3=x_{k+3}+x_{k+4}+\cdots+x_1+x_2$，

……

$S_n=x_n+x_1+\cdots+x_{k-1}$，$T_n=x_k+x_{k+1}+\cdots+x_{n-1}$，

（x_i 循环出现，在 x_n 的后面 x_1 重新出现）. 又令 $m(a,b)$ 为 i 的个数，使得 S_i 除以 3 余 a，T_i 除以 3 余 b，这里 a，b 为 0，1 或 2.

证明 $m(1,2)$ 与 $m(2,1)$ 除以 3 时余数相同.

2. （2008 年东南数学奥林匹克题）设正整数 m，$n\geqslant 2$，对于任一个 n 元整数集 $A=\{a_1,a_2,\cdots,a_n\}$，取每一对不同的数 a_i、$a_j(j>i)$，作差 a_j-a_i，由这 C_n^2 个差按从小到大顺序排成的一个数列，称为集合 A 的“衍生数列”，记为 $\overline{A}$. 衍生数列 $\overline{A}$ 中能被 m 整除的数的个数记为 $\overline{A}(m)$.

证明：对于任一正整数 $m\geqslant 2$，n 元整数集 $A=\{a_1,a_2,\cdots,a_n\}$ 及集合 $B=\{1,2,\cdots,n\}$所对应的“衍生数列”$\overline{A}$ 及 $\overline{B}$，满足不等式 $\overline{A}(m)\geqslant\overline{B}(m)$.

3. （2006 年女子数学奥林匹克题）设 p 为大于 3 的素数，求证：存在若干个整数 a_1，a_2，$\cdots$，a_t 满足条件

$-\frac{p}{2}<a_1<a_2<\cdots<a_t<\frac{p}{2}$,

使得乘积$\frac{p-a_1}{|a_1|}\cdot\frac{p-a_2}{|a_2|}\cdot\cdots\cdot\frac{p-a_t}{|a_t|}$是 3 的某个正整数次幂.

4. (2004 年国家队集训测试题) 若 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$, 其中 p_1, p_2, …, p_t 为不相同的素数, α_1, α_2, …, α_t 均为正整数, 则称 $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, …, $p_t^{\alpha_t}$ 中最大的一个为 n 的最大素数幂因子. 设 n_1, n_2, …, n_{10000} 为 10000 个互不相同的正整数, 并且 n_1, n_2, …, n_{10000} 的最大素数幂因子均相同. 证明: 存在整数 a_1, …, a_{10000}, 使得 10000 个等差数列$\{a_i, a_i+n_i, a_i+2n_i, a_i+3n_i, \cdots\}(i=1,2,\cdots,10000)$两两不相交.
5. (2002 年西部数学奥林匹克题) 设 α、β 为方程 $x^2-x-1=0$ 的两个根, 令

   $a_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}$, $n=1, 2, \cdots$.

   (1) 证明: 对任意正整数 n, 有 $a_{n+2}=a_{n+1}+a_n$;

   (2) 求所有正整数 a、b, $a<b$, 满足对任意正整数 n, 有 b 整除 a_n-2na^n.
6. (2004 年国家队培训题) 已知 a, b 是不同的正有理数, 使得存在无穷多个正整数 n, a^n-b^n 是正整数, 求证: a 和 b 也是正整数.
7. (1991 年国家集训队选拔试题) 设函数 f 对非负整数有定义, 且满足条件:

   $f(0)=0, f(1)=1$,

   $f(n+2)=23f(n+1)+f(n), n=0, 1, 2, \cdots$

   试证对任意 $m\in\mathbf{N}$, 都存在 $d\in\mathbf{N}$, 使得

   $m\mid f(f(n))\Leftrightarrow d\mid n$.
8. (CMO - 13 试题) 求所有大于 3 的自然数, 使得 $1+C_n^1+C_n^2+C_n^3$ 整除 2^{2000}.
9. (1998 年国家集训队选拔赛题) 任意给定 $h=2^r$ (r 是非负整数). 求满足以下条件的所有自然数 k: 对每个这样的 k, 存在奇自然数 $m>1$ 和自然数 n, 使得

   $k\mid m^h-1, m\mid n^{\frac{m^h-1}{k}}+1$.
10. (2003 年国家集训队选拔赛题) 设 $A\subseteq\{0,1,2,\cdots,29\}$满足: 对任何整数 k 及 A 中任意数 a、b (a、b 可以相同), $a+b+30k$ 均不是两个相邻整数之积. 试定出所有元素个数最多的 A.
11. (2007 年国家队集训测试题) 求所有的正整数对 (a, b), 满足: a^2+b+1 是一个素数的幂, a^2+b+1 整除 b^2-a^3-1, 且 a^2+b+1 不整除$(a+b-1)^2$.

第四章　奇数与偶数

【基础知识】

1. 若一个整数能被 2 整除，则这个整数叫偶数，若一个整数被 2 除余 1，则这个整数叫奇数.

奇数集合和偶数集合都是以 2 为模的同余类.

2. 奇数个奇数的和（或差）是奇数，偶数个奇数的和（或差）是偶数.

任意多个偶数的和（或差）为偶数.

一个奇数与一个偶数的和（或差）是奇数.

两个整数的和与差有相同的奇偶性.

3. 任意多个奇数的积是奇数.

若任意多个整数中至少有一个偶数，则它们的积是偶数.

4. 两个连续整数的积 $n(n+1)$ 是偶数.

5. 如果一个偶数被奇数整除，那么商必定是偶数.

【典型例题与基本方法】

例 1　（第 32 届俄罗斯数学奥林匹克题）黑板上写着乘积 $a_1 \cdot a_2 \cdot \cdots \cdot a_{100}$，其中 a_1，a_2，…，a_{100} 为正整数. 如果将其中的一个乘号改为加号（保持其余乘号），发现在所得的 99 个和数中有 32 个是偶数. 试问，在 a_1，a_2，…，a_{100} 中至多有多少个偶数?

解　33 个.

设在 a_1，a_2，…，a_{100} 中，最左面的一个偶数是 a_i，最右面的一个偶数是 a_k.

记 $X_j=a_1a_2\cdots a_j$，$Y_j=a_{j+1}a_{j+2}\cdots a_{100}$.

易知，当 $j=1$，2，…，$i-1$ 时，X_j 为奇数，Y_j 为偶数，此时，和数 X_j+Y_j 为奇数；当 $j=k$，$k+1$，…，100 时，X_j 为偶数，Y_j 为奇数，和数 X_j+Y_j 也为奇数.

只有当 $j=i$，$i+1$，…，$k-1$ 时，X_j、Y_j 都是偶数，和数 X_j+Y_j 方为偶数. 这就表明 $k-i=32$.

由于位于 a_i 与 a_k 之间的数既可为奇数，也可为偶数，只有当它们都是偶数时，在 a_1，a_2，…，a_{100} 中的偶数最多，所以，最多有 33 个偶数.

例 2 （2007 年土耳其国家队选拔考试题）求所有的正奇数 n，使得存在正奇数 x_1，x_2，…，x_n 满足 $x_1^2+x_2^2+\cdots+x_n^2=n^4$.

解 由于 n 为正奇数，故

$n^4\equiv1 \pmod 8$.

又由于 $x_i(1\leqslant i\leqslant n)$ 为正奇数，故

$x_i^2\equiv1 \pmod 8$.

因此，$n\equiv x_1^2+x_2^2+\cdots+x_n^2\equiv n^4\equiv1 \pmod 8$.

另一方面，若 $n\equiv1 \pmod 8$，则可找到满足条件的 x_1，x_2，…，x_n.

若 $n=1$，令 $x_1=1$，则 $n^4=1=x_1^2$.

若 $n=8k+1(k\in\mathbf{N}_+)$，则

$$\begin{aligned}n^4&=(8k+1)^4\\&=(8k-1)^4+(8k+1)^4-(8k-1)^4\\&=(8k-1)^4+[(8k+1)^2-(8k-1)^2]\cdot[(8k+1)^2+(8k-1)^2]\\&=(8k-1)^4+32k(128k^2+2)\\&=(8k-1)^4+4k(32k-1)^2+(16k-1)^2+(92k-1)\\&=(8k-1)^4+4k(32k-1)^2+(16k-1)^2+92(k-1)+91\\&=(8k-1)^4+4k(32k-1)^2+(16k-1)^2+(k-1)(9^2+3^2+1^2+1^2)+\\&\quad(9^2+3^2+1^2).\end{aligned}$$

因此，n^4 可以表示成 $1+4k+1+4(k-1)+3=8k+1=n$ 个奇数的平方和.

综上，所求结果为 $n=8k+1(k\in\mathbf{N})$.

例 3 （1998 年上海市数学竞赛题）设 $n\in\mathbf{N}$，且使 $37.5^n+26.5^n$ 为正整数，求 n 的值.

解 因 $37.5^n+26.5^n=\dfrac{1}{2^n}(75^n+53^n)$.

当 n 为正偶数时，

$75^n+53^n\equiv(-1)^n+1^n\equiv2 \pmod 4$，

此时 75^n+53^n 为 $4l+2$ 的数，从而 $37.5^n+26.5^n$ 不可能为正整数.

当 n 为正奇数时，

$$\begin{aligned}75^n+53^n&=(75+53)(75^{n-1}-75^{n-2}\times53+\cdots+53^{n-1})\\&=2^7(75^{n-1}-75^{n-2}\times53+\cdots+53^{n-1}).\end{aligned}$$

上式括号内共有 n 项，且每一项均为奇数，因而括号内是奇数个奇数之和为奇数.

于是正奇数 n 只能取 $n=1, 3, 5, 7$.

由以上可知，只有当 $n=1, 3, 5, 7$ 时，$37.5^n+26.5^n$ 是正整数.

例 4 （1984 年第 18 届全苏数学奥林匹克题）(1) 有 n 个整数，其积为 n，其和为 0，求证数 n 能被 4 整除.

(2) 设 n 是能被 4 整除的自然数，求证可以找到 n 个整数，使其积为 n，其和为 0.

证明 (1) 设 $a_1, a_2, \cdots, a_n$ 为 n 个整数，且满足题设条件：

$$a_1+a_2+\cdots+a_n=0, \quad ①$$

$$a_1a_2\cdot\cdots\cdot a_n=n. \quad ②$$

若 n 是奇数，则由②，所有的因数 $a_i(i=1, 2, \cdots, n)$ 都是奇数，而奇数个奇数之和应为奇数，而不能为 0，与①矛盾.

所以 n 必为偶数.

当 n 为偶数时，则由②知，必有一 a_j 为偶数，再由①知，除 a_j 外，至少还应有一个偶数，否则就出现奇数个奇数与一个偶数之和，不可能等于 0.

因此，在 a_i 中至少要有两个偶数，再由②，n 必能被 4 整除.

(2) 设 n 是 4 的倍数，且 $n=4k$，$k\in\mathbf{N}$.

当 k 为奇数时，

$$n=2\cdot(-2k)\cdot1^{3k-2}\cdot(-1)^k.$$

由于
$$\begin{aligned}&2+(-2k)+\underbrace{1+\cdots+1}_{(3k-2)\text{个}}+\underbrace{(-1)+\cdots+(-1)}_{k\text{个}}\\&=2-2k+3k-2-k\\&=0.\end{aligned}$$

所以可选 1 个 2，1 个 $-2k$，$3k-2$ 个 1 和 k 个 -1，这 $4k$ 个数满足要求.

当 k 为偶数时，

$$n=(-2)\cdot(-2k)\cdot1^{3k}\cdot(-1)^{k-2}.$$

由于

$$\begin{aligned}&(-2)+(-2k)+\underbrace{1+\cdots+1}_{3k\text{个}}+\underbrace{(-1)+\cdots+(-1)}_{(k-2)\text{个}}\\&=-2-2k+3k+2-k\\&=0.\end{aligned}$$

所以可选 1 个 -2，1 个 $-2k$，$3k$ 个 1 和 $k-2$ 个 -1，这 $4k$ 个数满足要求.

例 5 （2002—2003 年英国数学奥林匹克题）对于每个正整数 $n>1$，设 $p(n)$ 为 n 的最大素因子. 求满足下列条件的所有互不相同的正整数 x、y、z.

(1) x、y、z 是等差数列；

(2) $p(xyz)\leqslant 3$.

解 不妨假设 $x<y<z$，条件 (2) 表明 xyz 中只可能有素因子 2 和 3，且 x、y、z 均为 $2^a\times 3^b$ 的形式，其中 a、b 为非负整数.

设 $h=(x,y)$，$x'=\frac{x}{h}$，$y'=\frac{y}{h}$. 由条件 (1) 知 $z=2y-x$. 令 $z'=\frac{z}{h}$，所以，x'、y'、z'均为正整数，且仍满足条件 (1)、(2).

由于 x' 与 y' 互素，且 $x'+z'=2y'$，所以，y' 与 z' 也互素. 故$(x',z')=1$ 或 2.

若 y'既能被 2 整除，也能被 3 整除，则一定有 $x'=z'=1$，与 x、y、z 互不相等矛盾. 下面分三种情况讨论.

(i) $y'=1$，于是 $x'=1$，$z'=1$，与互不相等矛盾.

(ii) $y'=2^a$，$a>0$. 由于$(x',y')=(z',y')=1$,所以，设 $x'=3^k$，$z'=3^l$，于是有 $3^k+3^l=2^{a+1}$. 因为 $k<l$，故有 $3^k\mid 2^{a+1}$，$k=0$，$x'=1$，从而有 $3^l=2^{a+1}-1$，即有 $2^{a+1}\equiv 1(\bmod 3)$，故 a 是奇数. 设 $a=2n-1$，则有 $3^l=2^{2n}-1=(2^n-1)(2^n+1)$. 由于$(2^n-1,2^n+1)=1$,所以，$2^n-1=3^0=1$，即 $n=1$，$a=1$，$l=1$，故 $x'=1$，$y'=2$，$z'=3$.

(iii) $y'=3^a$，$a>0$. 设 $x'=2^k$，$z'=2^l$，则 $2^k+2^l=2\times 3^a$，即 $2^{k-1}+2^{l-1}=3^a$. 由 $k<l$，得 $k-1=0$，即 $k=1$，$x'=2$. 于是有 $2^{l-1}=3^a-1$，所以，$l\geqslant 2$. 若 $l>2$，则

$$2^{l-2}=\frac{3^a-1}{2}=\sum_{r=0}^{a-1}3^r\equiv\sum_{r=0}^{a-1}1^r=a\equiv 0(\bmod 2),$$

所以，a 是偶数，设 $a=2n$，于是有

$2^{l-1}=(3^n-1)(3^n+1)$.

故 $3^n-1=2$，$3^n+1=4$，$n=1$，$l=4$.

因此，$x'=2$，$y'=9$，$z'=16$.

若 $l=2$，则 $a=1$，所以，$x'=2$，$y'=3$，$z'=4$.

综上所述,$(x,y,z)=(h,2h,3h)$,$(2h,3h,4h)$或$(2h,9h,16h)$,其中 h 是形如 $2^a\times 3^b$ 的整数.

例 6 （2006 年法国国家队选拔考试题）求所有的三元整数组(a,b,c)，使得 $a^2+b^2=c^2$，$\gcd(a,b,c)=1$，$2000\leqslant a$、b、$c\leqslant 3000$.

解 由勾股数组(a,b,c)的特性知

$a=2pq$，$b=p^2-q^2$，$c=p^2+q^2$，

其中，p、$q(q<p)$是互素的正整数，且有一数为偶数.

由题设条件得

$c^2=a^2+b^2>2\times 2000^2$，

所以，$2000\sqrt{2}<c=p^2+q^2<3000$.

将$\sqrt{2}$的近似值 1.4142 代入上式得

$2828<p^2+q^2<3000$. ①

注意到 $2000<p^2-q^2$. ②

①+②得 $4828<2p^2$，所以，

$p\geqslant 50$. ③

注意到 $2000<2pq$. ④

①+④得$(p-q)^2<1000$，从而，

$p-q\leqslant 31$. ⑤

由式③⑤得 $q\geqslant 19$.

从而，$p^2+19^2\leqslant p^2+q^2<3000$，即 $p^2<2639$.

所以，$p\leqslant 51$.

于是，$2q=\frac{2pq}{p}>\frac{2000}{51}$，得 $q\geqslant 20$.

从而，$p^2+20^2\leqslant p^2+q^2<3000$，即 $p^2<2600$.

因而，$p\leqslant 50$.

故 $p=50$.

于是，$50^2+q^2<3000$，即 $q^2<500$.

因而，$q\leqslant 22$.

因为 p 为偶数，所以，q 一定为奇数.

因此，$q=21$.

易知 $a=2100$，$b=2059$，$c=2941$ 是满足要求的唯一三元数组.

例 7 （第 54 届白俄罗斯数学奥林匹克题）老师在黑板上写了 $n(n>2)$ 个正整数，这些数中任两个数不存在整除关系. 学生轮流擦去黑板上的某些数，使得每人恰好擦去一个数，且此数是该生离开前能整除黑板上余下所有数之和的数. 最后，黑板上恰好有两个数. 问：对任意 $n>2$ 是否均可能成立？

解 可能成立.

对任意 $n>2$，存在正整数 $a_1, a_2, \cdots, a_n$，使得

$$\begin{cases} a_3 \mid (a_1+a_2), \\ a_4 \mid (a_1+a_2+a_3), \\ \cdots\cdots \\ a_n \mid (a_1+a_2+\cdots+a_{n-1}), \end{cases} \quad ①$$

其中，$a_j \nmid a_i$，$i\neq j$.

定义 a_1，a_2，…，a_n 是数列

$$pq\quad 2,\ pq+2,\ 2pq,\ 4(p+0),4(q+1),4(p+1),\cdots,4(q+k),4(p+k),\cdots$$

的前 n 项，其中，p、q 是奇数，且

$$p>4n,\ q=(p+n)!\ +1.$$

易知，式①成立，且此数列中不存在任两项有整除关系．所以，a_1，a_2，…，a_n 为所求．

【解题思维策略分析】

1．根据所给奇、偶数条件分析

例 8　（2006 年泰国数学奥林匹克题）229 个男生和 271 个女生被平均分成 10 组，并用 1 到 50 标记每个组的学生．现选取 4 个学生（其中，含有奇数个女生），满足性质：他们来自两个组，且 4 个学生中有两对学生的号码相同．证明：满足要求的 4 人组的组数为奇数．

证明　将选自两个组且有 2 对相同号码的 4 个学生称为一个"队"．设

$S=\{\delta|\delta$ 是一个队$\}$，

$O=\{\delta\in S|\delta$ 含有奇数个女生$\}$，

$E=\{\delta\in S|\delta$ 含有偶数个女生$\}$．

只需证明：$|O|$ 为奇数．

对于所有的 S 的子集 A，定义

$f(A)=\sum\limits_{\delta\in A}\delta$ 中女生的人数．

由于 $O\cap E=\varnothing$，$O\cup E=S$，故

$f(S)=f(O)+f(E)$．

又因为 $f(E)$ 为偶数，所以，

$f(S)\equiv f(O)\pmod 2$．

$f(S)$ 可由如下方法求出：对于某个"指定"的女生，可从其所在组内选出另一名学生，共有 $50-1=49$ 种选法，再从其他 9 组中选出与这 2 名学生号码相同的学生．因此，每个女生可能在 49×9 个队里，也就是说，每个女生在 $f(S)$ 中被重复计数了 49×9 次．又因为女生共有 271 人，所以

$f(S)=49\times9\times271\equiv1\pmod 2$．

又每个 $\delta\in O$ 均有奇数个女生，则

$f(O)\equiv|O|\pmod 2$．

因此，$|O|=f(O)=f(S)\equiv1\pmod 2$．

故 $|O|$ 为奇数．

例 9 （1988 年全国高中数学联赛题）已知：$a_1=1$，$a_2=2$，

$$a_{n+2}=\begin{cases}5a_{n+1}-3a_n, & a_n\cdot a_{n+1}\text{为偶数时},\\ a_{n+1}-a_n, & a_n\cdot a_{n+1}\text{为奇数时}.\end{cases}$$

求证对一切 $n\in\mathbf{N}$，$a_n\neq 0$.

证法 1 因为 $a_1=1$，$a_2=2$，所以不防设 $a_{2k-1}=3p+1$，$a_{2k}=3q+2$，$(k\in\mathbf{N},p,q\in\mathbf{Z})$.

下面求 a_{2k+1}，则 a_{2k+1} 为下列两种情形的一种：

$$a_{2k+1}=5a_{2k}-3a_{2k-1}=5(3q+2)-3(3p+1)$$
$$=3(5q-3p+2)+1=3s'+1(s'\in\mathbf{Z}),$$

或 $$a_{2k+1}=a_{2k}-a_{2k-1}=(3q+2)-(3p+1)$$
$$=3(q-p)+1=3s''+1(s''\in\mathbf{Z}).$$

统一记为 $a_{2k+1}=3s+1$.

下面再计算 a_{2k+2}.

$$a_{2k+2}=5a_{2k+1}-3a_{2k}=5(3s+1)-3(3q+2)$$
$$=3(5s-3q-1)+2=3t'+2(t'\in\mathbf{Z}),$$

或 $$a_{2k+2}=a_{2k+1}-a_{2k}=(3s+1)-(3q+2)$$
$$=3(s-q-1)+2=3t''+2(t''\in\mathbf{Z}).$$

由以上知，在数列$\{a_n\}$中，奇数项被 3 除余 1，偶数项被 3 除余 2，即不会出现 3 的倍数的项，而 0 是 3 的倍数，所以 $a_n\neq 0$.

证法 2 设 $A_i=\{4k+i\mid k\in\mathbf{Z}\}, i=1,2,3.$

$a_1=1\in A_1$，$a_2=2\in A_2$，

$a_3=5a_2-3a_1=5\cdot 2-3\cdot 1=7\in A_3$.

假设 $a_{3m+1}\in A_1$，$a_{3m+2}\in A_2$，$a_{3m+3}\in A_3$，即有

$a_{3m+1}=4p+1$，$a_{3m+2}=4q+2$，$a_{3m+3}=4r+3$，

其中 p，q，$r\in\mathbf{Z}$. 于是

$$a_{3m+4}=5a_{3m+3}-3a_{3m+2}=4(5r-3q+2)+1\in A_1,$$
$$a_{3m+5}=a_{3m+4}-a_{3m+3}=4(4r-3q+1)+2\in A_2,$$
$$a_{3m+6}=5a_{3m+5}-3a_{3m+4}=4(5r-6q)+3\in A_3,$$

所以，对一切 $n\in\mathbf{N}$，

$a_n\in A_1\cup A_2\cup A_3$.

但 $0\notin A_1\cup A_2\cup A_3$，

所以 $a_n\neq 0$.

证法 3 由递推公式可知，a_n，a_{n+1}，a_{n+2}的奇偶性只能有奇，偶，奇；偶，奇，

奇；奇，奇，偶这三种情形.

由于 $a_1=1$，$a_2=2$，$a_3=7$ 都不是 4 的倍数，下面证明$\{a_n\}$中所有的项都不是 4 的倍数.

假设 a_m 是 4 的倍数，且 m 为最小下标，显然 $m>3$，则 a_{m-1}，a_{m-2}均为奇数，a_{m-3}为偶数.

$a_m=a_{m-1}-a_{m-2}$，

$a_{m-1}=5a_{m-2}-3a_{m-3}$，

于是 $3a_{m-3}=4a_{m-2}-a_m$.

则 a_{m-3}也是 4 的倍数，与 m 为 a_m 是 4 的倍数的最小下标矛盾.

因为 0 是 4 的倍数，所以对所有的 $n\in\mathbf{N}$，$a_n\neq 0$.

例 10 （1990 年全国高中数学联赛题）设 $E=\{1,2,3,\cdots,200\}$，$G=\{a_1,a_2,a_3,\cdots,a_{100}\}\subset E$，且 G 具有下列两条性质：

(i) 对任何 $1\leqslant i<j\leqslant 100$，恒有 $a_i+a_j\neq 201$.

(ii) $\sum\limits_{i=1}^{100}a_i=10080$.

试证明 G 中的奇数的个数是 4 的倍数，且 G 中所有数字的平方和为一个定数.

证法 1 由条件 (i)，$a_i+a_j\neq 201$，

所以在 G 中选了一个奇数 t，则 E 中的相应的偶数 $201-t$ 就必然不在 G 内.

由于 E 中 100 个偶数之和

$$2+4+\cdots+200=\frac{(2+200)\cdot 100}{2}=10100>10080,$$

则 G 中不可能全为偶数.

设 G 中有 k 个奇数，每个奇数设为 $2n_i-1(i=1,2,\cdots,k,n_i\in\mathbf{N})$.

从而必须从 E 中的 100 个偶数中除掉 k 个，每个偶数设为 $2m_i(i=1,2,\cdots,k,m_i\in\mathbf{N})$，且满足

$2n_i-1+2m_i=201$，即 $m_i+n_i=101$.

于是有

$$10100-(2m_1+2m_2+\cdots+2m_k)+[(2n_1-1)+(2n_2-1)+\cdots+(2n_k-1)]=10080.$$

$$\begin{aligned}20&=2(m_1-n_1+m_2-n_2+\cdots+m_k-n_k)+k\\&=2[(m_1+n_1)-2n_1+(m_2+n_2)-2n_2+\cdots+(m_k+n_k)-2n_k]+k\\&=2(101k-2n_1-2n_2-\cdots-2n_k)+k.\end{aligned}$$

即 $203k=20+4(n_1+n_2+\cdots+n_k)$.

因为 $(203,4)=1$，所以必有 $4\mid k$.

即 G 中奇数的个数是 4 的倍数.

又 $\sum_{i=1}^{100} a_i^2+\sum_{i=1}^{100}(201-a_i)^2=\sum_{i=1}^{200} i^2$,

$$2\sum_{i=1}^{100} a_i^2=\sum_{i=1}^{200} i^2-100\cdot 201^2+402\sum_{i=1}^{100} a_i$$
$$=\sum_{i=1}^{200} i^2-100\cdot 201^2+402\cdot 10080,$$

所以 $\sum_{i=1}^{100} a_i^2$ 是一个常数.

证法 2 把 E 分成$\{1,200\},\{2,199\},\cdots,\{100,101\}$共 100 个子集.

显然，集合 G 中的元素是从这 100 个子集中各取一个元素.

又可把这 100 个子集分成两类：

一类是

$\{1,200\},\{4,197\},\{5,196\},\{8,193\},\cdots$

这一类中每个子集中的两个元素一个为 $4k$ 型，一个为 $4k+1$ 型.

另一类是

$\{2,199\},\{3,198\},\{6,195\},\{7,194\},\cdots$

这一类中每个子集中的两个元素，一个为 $4k+2$ 型，一个为 $4k+3$ 型.

设集合 G 中的 100 个元素中 $4k+1$ 型的有 x 个，$4k+3$ 型的有 y 个，则 $4k$ 型的有 $50-x$ 个，$4k+2$ 型的有 $50-y$ 个.

这时，$x+y$ 即为 G 中奇数的个数. 因为

$$\sum_{i=1}^{100} a_i\equiv(4k+1)x+4k(50-x)+(4k+3)y+(4k+2)(50-y)$$
$$\equiv x+3y-2y\equiv x+y\equiv 10080\equiv 0 \pmod 4).$$

所以 $4\mid x+y$.

即 G 中的奇数的个数是 4 的倍数.

下面证明 G 中所有数的平方和是一个常数.

设 $G_1=\{a_1,a_2,\cdots,a_{100}\}$,

$G_2=\{b_1,b_2,\cdots,b_{100}\}$,

为满足条件的两个不同的集合，则有

$$\sum_{i=1}^{100} a_i=\sum_{i=1}^{100} b_i=10080.$$

不妨设 G_1，G_2 中不同的元素共有 k 个，记为 $a_{i_1},a_{i_2},\cdots,a_{i_k};b_{i_1},b_{i_2},\cdots,b_{i_k}$，其中 $a_{i_1}<a_{i_2}<\cdots<a_{i_k},b_{i_1}>b_{i_2}>\cdots>b_{i_k}$.

显然有

$a_{i_1}+b_{i_1}=a_{i_2}+b_{i_2}=\cdots=a_{i_k}+b_{i_k}=201.$

于是

$$\begin{aligned}\sum_{i=1}^{100}a_i^2-\sum_{i=1}^{100}b_i^2-\sum_{j=1}^{k}(a_{i_j}^2-b_{i_j}^2)&=\sum_{j=1}^{k}(a_{i_j}+b_{i_j})(a_{i_j}-b_{i_j})\\&=201\sum_{j=1}^{k}(a_{i_j}-b_{i_j})\\&=201\left(\sum_{j=1}^{k}a_{i_j}-\sum_{j=1}^{k}b_{i_j}\right)\\&=0.\end{aligned}$$

所以 $\sum_{i=1}^{100}a_i^2=\sum_{i=1}^{100}b_i^2.$

即 G 中所有数的平方和为一常数.

例 11 （1988 年国家集训队测验题）（1）求证存在正实数 λ，使得对任意正整数 n，$[\lambda^n]$和 n 有相同的奇偶性.

（2）求出一个满足（1）的正实数 λ.

解 令 λ 为方程

$$x^2-3x-2=0 \quad ①$$

的正根，则 $\lambda=\frac{3+\sqrt{17}}{2}$，$\mu=\frac{3-\sqrt{17}}{2}$，其中 μ 为方程①的负根，且满足 $-1<\mu<0$.

令 $S_n=\lambda^n+\mu^n$，则由①有

$\lambda^{n+2}-3\lambda^{n+1}-2\lambda^n=0,$

$\mu^{n+2}-3\mu^{n+1}-2\mu^n=0,$

即 $(\lambda^{n+2}+\mu^{n+2})-3(\lambda^{n+1}+\mu^{n+1})-2(\lambda^n+\mu^n)=0,$

$S_{n+2}-3S_{n+1}-2S_n=0(n\geqslant1).$

容易求出，$S_1=3,S_2=13.$

又 $S_{n+2}\equiv S_{n+1}(\bmod 2)$，则

$S_n\equiv1(\bmod 2).$

再由 $-1<\mu<0$ 及 $S_n=\lambda^n+\mu^n$ 可得

$$[\lambda^n]=\begin{cases}S_n=n(2\nmid n)(\bmod 2),\\S_n-1\equiv n(2\mid n)(\bmod 2).\end{cases}$$

例 12 （2003 年西部数学奥林匹克题）设 n 为给定的正整数，求最小的正整数

u_n，满足：对每一正整数 d，任意 u_n 个连续的正奇数中能被 d 整除的数的个数不小于奇数 1，3，5，…，$2n-1$ 中能被 d 整除的数的个数.

解 答案为 $u_n=2n-1$.

(1) 先证 $u_n\geqslant 2n-1$. 由于 $u_1\geqslant 1$，故不妨设 $n\geqslant 2$. 由于在 1，3，…，$2n-1$ 中能被 $2n-1$ 整除的数的个数为 1，在 $2(n+1)-1,2(n+2)-1,\cdots,2(n+2n-2)-1$ 中能被 $2n-1$ 整除的数的个数为 0，因此 $u_n\geqslant 2n-1$.

(2) 再证 $u_n\leqslant 2n-1$. 只要考虑 d 为奇数且 $1\leqslant d\leqslant 2n-1$ 的情形.

考虑 $2n-1$ 个奇数：$2(a+1)-1,2(a+2)-1,\cdots,2(a+2n-1)-1$. 设 s、t 为整数，使得

$$(2s-1)d\leqslant 2n-1<(2s+1)d,$$

$$(2t-1)d<2(a+1)-1\leqslant(2t+1)d,$$

则在 1，3，…，$2n-1$ 中能被 d 整除的数的个数为 s，所以只要证明

$$[2(t+s)-1]d\leqslant 2(a+2n-1)-1$$

即可. 事实上，有

$$\begin{aligned}(2(t+s)-1)d&=(2t-1)d+(2s-1)d+d\\&\leqslant 2(a+1)-1+2n-1+2n-1\\&=2(a+2n-1)-1,\end{aligned}$$

因此 $u_n\leqslant 2n-1$.

综上所述，得 $u_n=2n-1$.

注 本题的关键是发现在 $2(n+1)-1,2(n+2)-1,\cdots,2(n+2n-2)-1$ 这连续 $2n-2$ 个数中能被 $2n-1$ 整除的数的个数为 0，少于 $1,3,\cdots,2n-1$ 中能被 $2n-1$ 整除的数的个数，所以，得到 $u_n\geqslant 2n-1$. 于是，将问题归结为证明 $u_n\leqslant 2n-1$.

2. 分析题设条件中有关整数的奇偶性

例 13 (CMO-1 试题) 能否把 1，1，2，2，…，1986，1986 这些数排成一行，使得两个 1 之间夹着一个数，两个 2 之间夹着两个数，…，两个 1986 之间夹着一千九百八十六个数？请证明你的结果.

证法 1 不可能做到.

下面用反证法证明这个结论.

由题设，若能排成，设第一个数 k 写在第 a_k 位，第二个数 k 写在第 b_k 位，则必有 $b_k-a_k=k+1$.

取 $k=1$，2，…，1986，则

$$\sum_{k=1}^{1986}(b_k-a_k)=\sum_{k=1}^{1986}(k+1),$$

即 $\sum\limits_{k=1}^{1986}(b_k+a_k)-2\sum\limits_{k=1}^{1986}a_k=\sum\limits_{k=1}^{1986}(k+1)$.

$1+2+3+\cdots+1986+1987+\cdots+3972-2\sum\limits_{k=1}^{1986}a_k=2+3+4+\cdots+1986+1987$,

即 $\dfrac{3972\cdot 3973}{2}-2\sum\limits_{k=1}^{1986}a_k=\dfrac{1986\cdot 1989}{2}$,

即 $1986\cdot 3973-2\sum\limits_{k=1}^{1986}a_k=993\cdot 1989$.

此式左边为偶数，右边为奇数，显然不可能成立.

即题设所要求的排法不可能做到.

证法 2 考虑任一偶数对.

当一个偶数 k 占据第奇数位时，则另一个偶数 k 占据第偶数位，反之亦然.

考虑任一奇数对.

当一个奇数 t 占据第奇数位时，则另一个奇数 t 也占据第奇数位，或者当一个奇数 s 占据第偶数位时，则另一个奇数 s 也占据第偶数位.

由于 $2\cdot 1986$ 个位置中共有 1986 个奇数位、1986 个偶数位.

因为有 993 对偶数，所以共占据了 993 个奇数位.

而 993 对奇数占了偶数个（设为 $2m$）奇数位，于是

$993+2m=1986$.

这是不可能的.

所以题目要求的排法不可能做到.

证法 3 考察任何两个 a 和任何两个 b 相互被夹的关系.

容易看出，如果恰有一个 b 被夹在两个 a 之间，那么也恰有一个 a 被夹在两个 b 之间；

如果两个 b 都夹在两个 a 之间，那么就不会有 a 被夹在两个 b 之间；

而如果没有 b 被夹在两个 a 之间，那么或者没有 a 被夹在两个 b 之间，或者两个 a 都被夹在两个 b 之间.

由以上可以看出：任何两对不同数字相互被夹的数目之和不是 2 就是 0，即为偶数. 于是在两个 1，两个 2，…，两个 1986 之间被夹的其他数字的总数目一定是偶数，然而

$1+2+3+\cdots+1986=1987\cdot 993$

是奇数，出现矛盾.

所以题设所要求的排法不可能做到.

例 14 （2006 年西部数学奥林匹克题）设 $S=\{n\mid n-1、n、n+1$ 都可以表示为两

个正整数的平方和}. 证明：若 $n\in S$，则 $n^2\in S$.

证明 注意到若 x，y 是整数，则由奇偶性分析知

$x^2+y^2\equiv0,1,2 \pmod 4$.

若 $n\in S$，则由上知 $n\equiv1 \pmod 4$. 于是可设

$n-1=a^2+b^2, a\geqslant b$,

$n=c^2+d^2, c>d$（c,d 不可能相等），

$n+1=e^2+f^2, e\geqslant f$,

其中 a,b,c,d,e,f 都是正整数.

则 $n^2+1=n^2+1^2, n^2=(c^2+d^2)^2=(c^2-d^2)^2+(2cd)^2$,

$n^2-1=(a^2+b^2)(e^2+f^2)=(ae-bf)^2+(af+be)^2$.

假设 $b=a$，且 $f=e$，则 $n-1=2a^2, n+1=2e^2$，两式相减得 $e^2-a^2=1$，则 $e-a\geqslant1$，而 $1=e^2-a^2=(e+a)(e-a)>1$，矛盾！

故 $b=a, f=e$ 不可能同时成立. 所以 $ae-bf>0$，于是 $n^2\in S$.

例 15 （第 8 届香港数学奥林匹克题）求证：存在无穷多个不含平方因子的正整数 n，使得 $n\mid(2005^n-1)$.

证明 首先来看：如果 p 是 $a-1$ 的一个奇因子，那么，a^p-1 有一个不同于 p 的奇因子 q.

注意到

$$
\begin{aligned}
a^p-1&=(a-1)(a^{p-1}+a^{p-2}+\cdots+1)\\
&=kp[(kp+1)^{p-1}+(kp+1)^{p-2}+\cdots+1]\\
&=kp\{Ap^2+[(p-1)+(p-2)+\cdots+1]kp+p\}\\
&=kp^2\left[\left(A+\frac{p-1}{2}k\right)p+1\right],
\end{aligned}
$$

其中，$a-1=kp$，而 $\left(A+\frac{p-1}{2}k\right)p+1$ 有不同于 p 的因子.

下面证明 $\left(A+\frac{p-1}{2}k\right)p+1$ 有一个奇因子.

如果 a 是一个偶数，则 a^p-1 是一个奇数，因此，它的所有因子都是奇数.

如果 a 是一个奇数，则 k 是偶数，于是，A 也是偶数 [因为 Ap^2 是所有形如 $k^sp^s(s\geqslant2)$ 的数的和].

从而，$\left(A+\frac{p-1}{2}k\right)p+1$ 是奇数.

注意到 $2005-1=2004=2^2\times3\times167$.

令 $p_1=3$，则 $3\mid(2005-1)$ 且 $3\mid(2005^3-1)$.

根据前面的结论，可以找到一个奇素数 $p_2(p_2\neq3)$，使得 $p_2\mid(2005^3-1)$，于是，

$p_1p_2\mid(2005^{p_1p_2}-1)$.

再次使用前面的结论，又可以找到一个奇素数 $p_3(p_3\neq p_1、p_2)$使得 $p_3\mid(2005^{p_1p_2}-1)$. 于是，

$p_1p_2p_3\mid(2005^{p_1p_2p_3}-1)$.

这样一来，就构造出了无穷多个符合条件的 n：$(p_1,p_1p_2,p_1p_2p_3,\cdots)$，使得

$n\mid(2005^n-1)$.

显然，它们没有平方因子且两两不同.

例 16 （第 34 届俄罗斯数学奥林匹克题）令 p 是一个由有限个素数组成的集合. 证明：存在正整数 x，使得 x 可以表示为两个正整数的素数次幂的和当且仅当这个素数属于 p.

证明 首先来看如下引理.

引理 设 p 是一个素数，n 为一个正整数，则存在正整数 a、b，使得 $2^n=a^p+b^p$ 当且仅当 $p\mid(n-1)$.

引理的证明：如果 $n-1=kp$，则

$2^n=(2^k)^p+(2^k)^p$.

反过来，若 $2^n=a^p+b^p$，设 $a=2^sk$，$b=2^tl$，其中，k、l 为奇数.

如果 $s>t$，则

$2^n=a^p+b^p=2^{pt}[2^{p(s-t)}k^p+l^p]$.

由于 $2^{p(s-t)}k^p+l^p$ 是一个大于 1 的奇数，这是不可能的. 故

$s=t$，$a^p+b^p=2^{pt}(k^p+l^p)$.

如果 $p=2$，则 $k^p+l^p\equiv2\pmod 4$. 故只要 $k^p+l^p>2$，2^n 就有一个大于 1 的奇因数$\frac{k^p+l^p}{2}$，矛盾. 由此推出 $k=l=1$，$2^n=2\times2^{pt}$，得到 $n=pt+1$.

如果 $p>2$，则

$k^p+l^p=(k+l)(k^{p-1}-k^{p-2}l+\cdots+l^{p-1})$.

上式右端第二个括号里是一个奇数，故它必等于 1，这推出 $k^p+l^p=k+l$.

因此，$k=l=1$，$n=pt+1$.

回到原题.

设 $p=\{p_1,p_2,\cdots,p_n\}$，令 $x=2^{p_1p_2\cdots p_n+1}$，由引理，这个数满足要求.

例 17 （2002—2003 年度英国数学奥林匹克题）求所有正整数 a、b、c，使得 a、b、c 满足

$(a!)(b!)=a!+b!+c!$.

解 不失一般性，假设 $a \geqslant b$，则原方程化为 $a! = \frac{a!}{b!}+1+\frac{c!}{b!}$.

由于上式中有三项是整数，所以 $c \geqslant b$.

又因为右边的每一项都是正整数，则其和至少是 3. 因此，$a \geqslant 3$，且 $a!$ 是偶数.

于是，$\frac{a!}{b!}$和$\frac{c!}{b!}$中有且仅有一项是奇数.

(1) 假设$\frac{a!}{b!}$是奇数，则要么 $a=b$，要么$\frac{a!}{b!}=b+1$，且 $b+1$ 是奇数，$a=b+1$.

(i) 若 $a=b$，则 $a! =2+\frac{c!}{a!}$.

当 $a=3$ 时，有 $b=3$，$c=4$.

当 $a>3$ 时，由于 $a! -2$ 不能被 3 整除，所以，

$c=a+1$ 或 $a+2$，

$\frac{c!}{a!}=a+1$ 或$(a+1)(a+2)$，

$a! =a+3$ 或$(a+1)(a+2)+2$. ①

当 $a=4$ 或 5 时，不满足方程.

当 $a \geqslant 6$ 时，明显式①左边大于右边，此时原方程无解.

(ii) 若 $a=b+1$，其中 b 是偶数，则原方程化为

$(b+1)! =b+2+\frac{c!}{b!}$.

上式左端可以被 $b+1$ 整除，由于$\frac{a!}{b!}$为奇数时，$\frac{c!}{b!}$为偶数，故 $c>b$. 于是$\frac{c!}{b!}$可以被 $b+1$ 整除，所以，$b+2$ 可以被 $b+1$ 整除. 矛盾.

(2) 假设$\frac{a!}{b!}$是偶数，$\frac{c!}{b!}$是奇数，则 $c=b$ 或 $c=b+1$（b 为偶数).

(i) 若 $c=b$，则方程化为

$(a!)(b!)=(a!)+2\times(b!)$.

所以，$\frac{a!}{b!}(b! -1)=2$.

故$\frac{a!}{b!}=2, b! -1=1$.

于是，$b=2, a! =4$，不可能.

(ii) 若 $c=b+1$，则方程化为$(a!)(b!)=(a!)+(b+2)(b!)$.

所以，$a! (b! -1)=(b+2)(b!)$.

由于$(b!,b!-1)=1$，因此，

$(b!-1)|(b+2)$.

因为b是偶数，所以，$b=2$，$a!=8$，不可能.

综上所述，原方程有唯一解$a=3$，$b=3$，$c=4$.

例 18 （2008年东南数学奥林匹克题）设n为正整数，$f(n)$表示满足以下条件的n位数（称为波形数）$\overline{a_1a_2\cdots a_n}$的个数：

(i) 每一位数码$a_i\in\{1,2,3,4\}$，且$a_i\neq a_{i+1}$，$i=1,2,\cdots$；

(ii) 当$n\geqslant3$时，a_i-a_{i+1}与$a_{i+1}-a_{i+2}$的符号相反，$i=1,2,\cdots$.

(1) 求$f(10)$的值；

(2) 确定$f(2008)$被13除得的余数.

解 当$n\geqslant2$时，称满足$a_1<a_2$的n位波形数$\overline{a_1a_2\cdots a_n}$为$A$类数，其个数为$g(n)$；而满足$a_1>a_2$的$n$位波形数$\overline{a_1a_2\cdots a_n}$为$B$类数，据对称性，当$n\geqslant2$时，其个数也是$g(n)$，于是$f(n)=2g(n)$.

今求$g(n)$：用$m_k(i)$表示末位为i的k位A类波形数的个数$(i=1,2,3,4)$，则

$$g(n)=\sum_{i=1}^{4}m_n(i).$$

由于$a_{2k-1}<a_{2k}$，$a_{2k}>a_{2k+1}$，则

(1) 当k为偶数时，

$m_{k+1}(4)=0$，$m_{k+1}(3)=m_k(4)$，$m_{k+1}(2)=m_k(4)+m_k(3)$，

$m_{k+1}(1)=m_k(4)+m_k(3)+m_k(2)$； ①

(2) 当k为奇数时，

$m_{k+1}(1)=0$，$m_{k+1}(2)=m_k(1)$，$m_{k+1}(3)=m_k(1)+m_k(2)$，

$m_{k+1}(4)=m_k(1)+m_k(2)+m_k(3)$， ②

易知$m_2(1)=0$，$m_2(2)=1$，$m_2(3)=2$，$m_2(4)=3$，则$g(2)=6$.

由此可得，

$m_3(1)=m_2(2)+m_2(3)+m_2(4)=6$，

$m_3(2)=m_2(3)+m_2(4)=5$，

$m_3(3)=m_2(4)=3$，$m_3(4)=0$，

所以 $g(3)=\sum_{i=1}^{4}m_3(i)=14$.

又由

$m_4(1)=0$，$m_4(2)=m_3(1)=6$，

$m_4(3)=m_3(1)+m_3(2)=11$，

$m_4(4)=m_3(1)+m_3(2)+m_3(3)=14$，

所以 $g(4)=\sum_{i=1}^{8} m_4(i)=31.$

类似可求得，$g(5)=70$，$g(6)=157$，$g(7)=353$，$g(8)=793$.

一般地，当 $n\geqslant 5$ 时，

$$g(n)=2g(n-1)+g(n-2)-g(n-3). \quad ③$$

今证③如下：

对 n 归纳，$n=5$，6，7，8 皆已验证，设③直至 n 皆成立，考虑 $n+1$ 情况.

当 n 为偶数时，根据 (1)、(2) 可得

$m_{n+1}(4)=0, m_{n+1}(3)=m_n(4), m_{n+1}(2)=m_n(4)+m_n(3),$

$m_{n+1}(1)=m_n(4)+m_n(3)+m_n(2),$

而 $m_n(1)=0$，则

$$\begin{aligned}g(n+1)&=\sum_{i=1}^{4} m_{n+1}(i)=2\Big(\sum_{i=1}^{4} m_n(i)\Big)+m_n(4)-m_n(2)\\&=2g(n)+m_n(4)-m_n(2).\end{aligned}$$

因为

$$\begin{aligned}m_n(4)&=m_{n-1}(1)+m_{n-1}(2)+m_{n-1}(3)+0\\&=\sum_{i=1}^{4} m_{n-1}(i)=g(n-1),\end{aligned}$$

$$\begin{aligned}m_n(2)&=m_{n-1}(1)=m_{n-2}(4)+m_{n-2}(3)+m_{n-2}(2)+0\\&=g(n-2),\end{aligned}$$

这时有 $g(n+1)=2g(n)+g(n-1)-g(n-2).$

当 n 为奇数时，$g(n+1)=\sum_{i=1}^{8} m_{n+1}(i)$，而

$m_{n+1}(1)=0, m_{n+1}(2)=m_n(1), m_n(4)=0,$

$m_{n+1}(3)=m_n(1)+m_n(2), m_{n+1}(4)=m_n(1)+m_n(2)+m_n(3),$

则 $$\begin{aligned}g(n+1)&=\sum_{i=1}^{4} m_{n+1}(i)=2\sum_{i=1}^{4} m_n(i)+m_n(1)-m_n(3)\\&=2g(n)+m_n(1)-m_n(3).\end{aligned}$$

因为

$m_n(1)=m_{n-1}(4)+m_{n-1}(3)+m_{n-1}(2)+0=g(n-1),$

$m_n(3)=m_{n-1}(4)=m_{n-2}(1)+m_{n-2}(2)+m_{n-2}(3)+0=g(n-2),$

这时也有

$g(n+1)=2g(n)+g(n-1)-g(n-2),$

故③式对于 $n+1$ 也成立，从而由归纳法得，对所有 $n\geqslant 5$，③式皆成立.

据③得

$g(9)=2g(8)+g(7)-g(6)=1782$,

$g(10)=2g(9)+g(8)-g(7)=4004$,

所以 $f(10)=2g(10)=8008$.

今考虑$\{g(n)\}$的模数列：

利用③式易算出，当$n=2,3,4,\cdots,14,15,16,17,\cdots$时，$g(n)$被13除得的余数分别是：

6, 1, 5, 5, 1, 2, 0, 1, 0, 1, 1, 3; 6, 1, 5, 5, …,

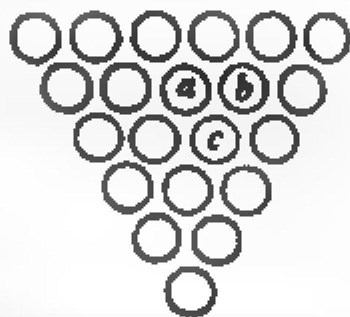
因此当$n\geqslant 2$时，数列$\{g(n)\}$被13除得的余数所构成的数列是一个周期数列，其最小周期长度为12. 而$2008=12\times 167+4$，所以

$g(2008)\equiv 5 \pmod{13}$,

因此，$f(2008)\equiv 10 \pmod{13}$.

3. 将问题转化运用奇偶分析求解

例19 (1990年第16届全俄数学奥林匹克题) 试问：能否将1至21这21个自然数分别填入图中的各个圆圈内，使得除第一行外，每个圆圈内的数字都等于其肩膀上两个圆圈内的数字之差的绝对值（亦即$c=|a-b|$，如下图).



解 假定我们已按照要求将1至21填入图中的各个圆圈之内.

由于两个数的和与这两个数的差有相同的奇偶性，我们考察另一种填法.

不改变第一行中6个圆圈上的数，而将第二行中的各个数都换成其两个肩膀上的数的和，并依照此法，再将第三行中的各个数都换成现在第二行中的位于其两个肩膀上的数的和，如此下去，将其余各行数重新换过.

这时，表中所填的各数的奇偶性都与原来所填的数相同.

于是，新填的表中所有数之和的奇偶性应当与和数$1+2+\cdots+21=231$相同，即为奇数.

然而，若第一行数为a, b, c, d, e, f，则按新填法

第二行为：$a+b$, $b+c$, $c+d$, $d+e$, $e+f$,

第三行为：$a+2b+c$, $b+2c+d$, $c+2d+e$, $d+2e+f$,

第四行为：$a+3b+3c+d$, $b+3c+3d+e$, $c+3d+3e+f$,

第五行为：$a+4b+6c+4d+e$, $b+4c+6d+4e+f$,

第六行为：$a+5b+10c+10d+5e+f$.

这时，所有数之和为$6a+20b+34c+34d+20e+6f$是偶数. 出现矛盾.

因此，不存在符合要求的填法.

例 20 （1989 年全国高中数学联赛题）有 $n\times n(n\geqslant 4)$的一张空白方格表，在它的每一个方格内任意地填入 $+1$ 与 -1 两个数中的一个. 现将表内 n 个两两既不同行（横）又不同列（竖）的方格中的数的乘积称为一个基本项.

试证：按上述方式所填成的每一个方格表，它的全部基本项之和总能被 4 整除（即总能表示成 $4k$ 的形式，其中 $k\in\mathbf{Z}$).

证法 1 显然，不论用怎样的填法，所填成的方格表总有 $n!$ 个基本项.

用 a_{ij} 表示方格表中第 i 行第 j 列的方格内所填的数，这里 $1\leqslant i, j\leqslant n$，$n\geqslant 4$，$i, j\in\mathbf{N}$.

现在考察一张已填成的方格表，记它的全部基本项之和为 S.

由题意，表中每个格内的数 a_{ij} 只能是 $+1$ 或 -1，而 $+1$ 与 -1 之间只相差一个负号，因此，当把方格表中的某一个数 a_{ij} 改变选择（即把 $+1$ 换成 -1 或把 -1 换成 $+1$）时，由于 a_{ij} 出现在和式 S 的$(n-1)!$ 个基本项中，由 $n\geqslant 4$，则 S 中将有偶数个基本项同时变号.

再注意到在 $n!$（偶数）个基本项中，值为 1 的基本项与值为 -1 的基本项的个数之差必为偶数，而 a_{ij} 在变号时，其所在的基本项的改变值是 2 或 -2，所以当某个 a_{ij} 改变选择时，引起 S 的改变值一定是 4 的倍数.

若一张方格表的所有 a_{ij} 全为 $+1$，则全部基本项之和 $S=n!$ $(n\geqslant 4)$显然能够被 4 整除. 若 a_{ij} 不全为 $+1$，则这张方格表可由一张 a_{ij} 全为 1 的方格表将相应方格中的数 $+1$ 经有限次变号而得到. 根据以上的讨论，每次变号均使基本项之和的改变值能被 4 整除.

从而无论用怎样的填法，所填成的方格表的全部基本项之和总能被 4 整除.

证法 2 设每个基本项为 x_i，则 x_i 只能取 $+1$ 或 -1，且基本项共有 $n!$ 个.

表中第 i 行，第 j 列的数记为 a_{ij}，则 a_{ij} 只能为 $+1$ 或 -1.

又因为方格表中每一个数 a_{ij} 都取了$(n-1)!$ 次，所以有

$$x_1x_2\cdots x_{n!}=\prod_{1\leqslant i,j\leqslant n}a_{ij}^{(n-1)!}.$$

由于 $n\geqslant 4$，所以 $2\mid(n-1)!$，因而

$a_{ij}^{(n-1)!}=1$，即 $x_1x_2\cdots x_{n!}=1$.

故在 x_1，x_2，…，$x_{n!}$ 中只可能有偶数个 -1，设有 $2k$ 个 -1，则有 $n!-2k$ 个 $+1$.

于是 $\sum\limits_{i=1}^{n!}x_i=(n!-2k)+(-1)\cdot 2k=n!-4k$.

又因为 $n\geqslant 4$，所以 $4\mid n!$，即 $4\mid n!-4k$，于是 $4\mid \sum\limits_{i=1}^{n!}x_i$.

例 21 （2006年保加利亚国家数学奥林匹克题）考察集合 $A=\{1,2,3,4,\cdots,2^n\}$，其中，$n\geqslant 2$. 如果集合 A 中两个元素的和是 2 的幂，那么，它们之中的一个恰好属于子集 B. 求集合 A 中子集 B 的个数.

解 设 B 是满足题设性质的一个子集. 因为 $1+3=2^2$，所以，1 或 3 恰好属于 B.

若 $1\in B$，则 $3\notin B$.

下面用数学归纳法证明：

对于任意一个整数 $t(0\leqslant t<2^{n-2})$，$4t+1$ 型的整数属于 B，$4t+3$ 型的整数不属于 B.

对于 $t=0$，结论显然成立.

假设对于 $t\leqslant s$，结论成立.

因为 $4(s+1)+1$ 为奇数，故存在 l 使得

$2^l<4(s+1)+1<2^{l+1}$.

所以，$2(4s+5)>2\times 2^l=2^{l+1}$.

从而，$0<2^{l+1}-(4s+5)<(4s+5)$.

令 $x=4s+5$，$y=2^{l+1}-(4s+5)$，则

$x+y=2^{l+1}$.

因为 y 是 $4m+3$ 型的整数，故

$y\notin B$，$4(s+1)+1\in B$.

类似地，$4(s+1)+3\notin B$.

若 $1\notin B$，则 $3\in B$.

同上可证，$4t+1$ 型的整数不属于 B，$4t+3$ 型的整数属于 B.

因此，子集 B 中的奇数或者是所有 $4t+1$ 型的整数或者是所有 $4t+3$ 型的整数.

设 $x=2^p x_0$，$y=2^q y_0$，其中 x_0、y_0 是奇数，p、q 是正整数.

如果 $2^p x_0+2^q y_0=2^k$，$p\neq q$，不失一般性，假设 $p<q$，则 $x_0+2^{q-p}y_0=2^{k-p}$ 是不可能的，所以，$p=q$. 由此得，取自不同集合 $A_i=\{2^i a\mid a \text{ 为奇数}\}(i=1,2,\cdots,n)$ 的元素的和不是 2 的幂.

对于任一个 A_i，除以 2^i 并由上面的讨论知，所有形如 $2^i(4t+1)$ 的整数在 B 中或所有形如 $2^i(4t+3)$ 的整数在 B 中.

因此，存在 2^{n+1} 个满足题设要求的子集 B.

例 22 （第37届加拿大数学奥林匹克题）若有序三元正整数组 $\{a,b,c\}$ 满足 $a\leqslant b\leqslant c$，$(a,b,c)=1$，$a^n+b^n+c^n$ 能被 $a+b+c$ 整除，则称 $\{a,b,c\}$ 是 n－能量的. 例如 $\{1,2,2\}$ 是 5－能量的.

(1) 求出所有的有序三元正整数组，满足：对于任意 $n\geqslant1$，其有序三元正整数组是 n—能量的；

(2) 求出所有既是 2004—能量的，又是 2005—能量的，但不是 2007—能量的有序三元正整数组.

解 (1) 因为$(a+b+c)\mid(a^2+b^2+c^2)$，$(a+b+c)\mid(a^3+b^3+c^3)$，则

$(a+b+c)\mid[(a+b+c)^2-a^2-b^2-c^2]$，即

$(a+b+c)\mid(2ab+2bc+2ca)$.

又$(a+b+c)(a^2+b^2+c^2-ab-bc-ca)=a^3+b^3+c^3-3abc$，故

$(a+b+c)\mid3abc$.

设素数 p 满足 $p^{\alpha}\parallel(a+b+c)(\alpha\geqslant1)$.

若存在 $p\geqslant5$，则 $p\mid abc$. 不妨设 $p\mid a$.

因为 $p\mid2(ab+bc+ca)$，所以 $p\mid bc$.

不妨设 $p\mid b$. 因为 $p\mid(a+b+c)$，所以 $p\mid c$.

则 $p\mid(a,b,c)$，矛盾.

所以，$p=2$ 或 3.

故 $a+b+c=2^m\times3^n(m、n\geqslant0)$.

若 $n\geqslant2$，则

$3\mid(a+b+c)$，$3\mid abc$，$3\mid(ab+bc+ca)$.

仿上即可推出 $3\mid(a,b,c)$，矛盾.

故 $n=0$ 或 1.

设 $a+b+c=2^mk(k=1$ 或 $3)$，则 $2^m\mid abc$.

因为$(a,b,c)=1$，不妨设 a 为奇数.

又 $2^m\mid(a+b+c)$，不妨设 b 为奇数，c 为偶数，所以，$2^m\mid c$.

由 $2^m\mid(2ab+2bc+2ca)$，则

$2^{m-1}\mid ab$.

从而，$m=0$ 或 1.

又 $a+b+c\geqslant3$，所以，$a+b+c=3$ 或 6.

分别验证得

$(a,b,c)=(1,1,1)$或$(1,1,4)$.

(2) 易得

$$a^n+b^n+c^n=(a+b+c)(a^{n-1}+b^{n-1}+c^{n-1})-(ab+bc+ca)(a^{n-2}+b^{n-2}+c^{n-2})+abc(a^{n-3}+b^{n-3}+c^{n-3}). \quad ①$$

又$(a+b+c)\mid(a^{2004}+b^{2004}+c^{2004})$，

$(a+b+c)\mid(a^{2005}+b^{2005}+c^{2005})$，

将 $n=2007$ 代入式①得

$(a+b+c)\mid(a^{2007}+b^{2007}+c^{2007})$，与条件矛盾.

故不存在满足条件的 (a,b,c).

例 23 （2007 年保加利亚数学奥林匹克题）求最大的正整数 n 满足：在区间 $[2\times10^{n-1},10^n)$ 内可以选取 2007 个不同的整数，使得对任意的 i、$j(1\leqslant i<j\leqslant n)$ 都存在一个被选出的数 $\overline{a_1a_2\cdots a_n}$，有 $a_j\geqslant a_i+2$.

解 考虑 2007 个满足题目要求的正整数.

将这 2007 个正整数中的每个数的所有是偶数的数码加 1，得到 2007 个“新的”正整数，且每个正整数的数码都是奇数（可能有些数没有改变，有些数会相等）.

若 a_i、a_j 奇偶性相同，则当它们同奇时，a_i，a_j 没有变化；当它们同偶时，a_i，a_j 分别变为 a_i+1，a_j+1.

若 a_i，a_j 奇偶性不同，则 a_j，a_i+2 的奇偶性也不同.

因此，$a_j\geqslant a_i+2$.

实际上，满足 $a_j>a_i+2$. 从而，当偶数的数码增加 1 后，满足条件的不等式仍然成立. 于是，这 2007 个新的正整数也满足题目的要求.

将这 2007 个数写在 $2007\times n$ 的表格内，使得每一行对应着一个数，并依次将每个数码写在一个方格内. 因此，第 1 列方格内的数至少是 3. 为满足要求，后面的每一列中至少有一个数比 3 大，因此，没有一列只包含 1 和 3. 于是，包含 1，3，5，7，9 的列有 5^{2007} 种取法，包含 1，3 的列有 2^{2007} 种取法，第 1 列可以全取 3. 因此，最多有 $1+5^{2007}-2^{2007}$ 列，即 $n\leqslant1+5^{2007}-2^{2007}$.

下面构造一个 $2007\times(1+5^{2007}-2^{2007})$ 的表格，使得每个方格内写一个数码. 每行数对应着一个数，这 2007 个数满足题目的要求.

在第 1 行依次写 5^{2006} 个 1，5^{2006} 个 3，5^{2006} 个 5，5^{2006} 个 7，5^{2006} 个 9；

在第 2 行依次写 5^{2005} 个 1，5^{2005} 个 3，5^{2005} 个 5，5^{2005} 个 7，5^{2005} 个 9，共重复写 5 遍；

在第 3 行依次写 5^{2004} 个 1，5^{2004} 个 3，5^{2004} 个 5，5^{2004} 个 7，5^{2004} 个 9，共重复写 5^2 遍；

……

在第 2007 行依次写 1 个 1，1 个 3，1 个 5，1 个 7，1 个 9，共重复写 5^{2006} 遍.

则对于任意的 i、$j(1\leqslant i<j\leqslant5^{2007})$，考虑第 i 列和第 j 列：从上到下第一次出现在某行的两个数不同，这两个数 a_i、a_j 一定满足 $a_j>a_i$. 于是 $a_j\geqslant a_i+2$.

上述 2007×5^{2007} 表格中每一行表示的 n 位数（其每位数码都是奇数）满足条件，

但其没有限制在区间$[2\times10^{n-1},10^{n})$内，其中，$n=5^{2007}$.

删去只包含 1 和 3 的列，并在第 1 列加上全是 3 的列，则共有 $1+5^{2007}-2^{2007}$ 列，满足题目的要求.

【模拟实战】

1. （2002 年全国女子数学奥林匹克题）夏令营有 $3n$（n 是正整数）位女同学参加，每天都有 3 位女同学担任值勤工作. 夏令营结束时，发现这 $3n$ 位女同学中的任何两位，在同一天担任值勤工作恰好是一次.
   (1) 问：当 $n=3$ 时，是否存在满足题意的安排？证明你的结论.
   (2) 求证：n 是奇数.
2. （2007 年俄罗斯数学奥林匹克题）对于整数 $n>3$，我们用 $n?$ 表示所有小于 n 的素数的乘积（称为“n－问号”）. 试解方程 $n?=2n+16$.
3. （IMO－26 预选题）x_1，x_2，…，x_n 为 $+1$ 或 -1，并且 $x_1x_2x_3x_4+x_2x_3x_4x_5+x_3x_4x_5x_6+\cdots+x_{n-3}x_{n-2}x_{n-1}x_n+x_{n-2}x_{n-1}x_nx_1+x_{n-1}x_nx_1x_2+x_nx_1x_2x_3=0$. 证明 n 能被 4 整除.
4. （2007 年克罗地亚数学竞赛题）已知数列$\{a_n\}$满足
   $a_0=3,a_n=2+a_0a_1\cdots a_{n-1}(n\geqslant1)$.
   (1) 证明：数列$\{a_n\}$的任意两项互素；
   (2) 求 a_{2007}.
5. （第 19 届北欧数学竞赛题）求所有正整数 k，使得在十进制表示下，k 的各位数字的积等于$\frac{25}{8}k-211$.
6. （2005 年新西兰奥林匹克选拔赛题）求所有正整数 x，y，使得$(x+y)(xy+1)$是 2 的整数次幂.
7. （2005 年克罗地亚数学竞赛题）求证：存在唯一由十进制表示的正整数，该数是仅由数字 2 和 5 组成的 2005 位数，且能被 2^{2005} 整除.
8. （第 17 届北欧数学竞赛题）我们将一些石头放入 10 行 14 列的矩形棋盘内，允许在每个单位正方形内放入石头的数目多于 1 块，然后发现在每一行每一列上均有奇数块石头. 如果将棋盘上的单位正方形相间地染为黑色和白色，证明：在黑色正方形上石头的数目共有偶数块.
9. （2007 年克罗地亚数学竞赛题）是否存在这样的直角三角形，其斜边长为$\sqrt{2006}$，两条直角边长均为整数？
10. （第 32 届俄罗斯数学奥林匹克题）对于怎样的正整数 n，可以找到两个非整数的

正有理数 a，b，使得 $a+b$ 与 a^n+b^n 都是整数？

11. （2004 2005 年度匈牙利数学奥林匹克题）已知 n 是正整数．如果存在整数 a_1，a_2，…，a_n（不一定是不同的）使得 $a_1+a_2+\cdots+a_n=a_1a_2\cdots a_n=n$，则称 n 是“迷人的”．求迷人的整数．

12. （第 20 届爱尔兰数学奥林匹克题）已知 r、n 均为非负整数，且 $r\leqslant n$．证明：

(1) $\dfrac{n+1-2r}{n+1-r}C_n^r$ 为整数；

(2) 对 $n\geqslant 9$，有 $\sum\limits_{r=0}^{\left[\frac{n}{2}\right]}\dfrac{n+1-2r}{n+1-r}C_n^r<2^{n-2}$，其中，$[x]$表示不超过实数 x 的最大整数．

13. （2003 年台湾集训营题）对于正整数 $n\geqslant 1$，设 $f(n)=k$，其中 $2^k\mid n$，$2^{k+1}\nmid n$．设 $x_0=0$，当 $n\geqslant 1$ 时定义 x_n 如下：$\dfrac{1}{x_n}=1+2f(n)-x_{n-1}$．

证明：每个非负有理数在数列 x_0，x_1，x_2，…中出现且仅出现一次．

14. （2003 年国家队培训题）如果一个正整数的所有正约数之和为其两倍，则称该数为一个完全数．求所有的正整数 n，使得 $n-1$ 和 $\dfrac{n(n+1)}{2}$ 都是完全数．

第五章　素数、合数及威尔逊定理

【基础知识】

1. 一个大于 1 的整数，如果只有 1 和它本身作为它的约数，这样的正整数叫做素数（也叫质数）. 如果除了 1 和它本身之外还有其他的正约数，这样的正整数叫做合数.

1 既不是素数也不是合数.

因此，自然数集 N 满足 N={1}∪{素数}∪{合数}.

2. 大于 1 的整数的所有真约数中，最小的正约数一定是素数.

3. 合数 a 的最小素约数不大于$\sqrt{a}$.

4. 素数有无穷多个.

5. 不存在这样的多项式 $f(n)=\sum_{i=0}^{m}a_in^i$，使得对任意的自然数 n，$f(n)$都是素数.

6. **威尔逊定理**：p 为素数的充分必要条件是$(p-1)!\equiv-1(\bmod p)$.

【典型例题与基本方法】

例 1　（1990 年第 24 届全苏数学奥林匹克题）试问，对于哪些自然数 n，数 $3^{2n+1}-2^{2n+1}-6^n$ 是合数.

解　原式可化为

$$\begin{aligned}3^{2n+1}-2^{2n+1}-6^n&=3^{2n+1}-3^n\cdot2^n-2^{2n+1}\\&=3^{2n+1}-3^{n+1}\cdot2^n+3^n\cdot2^{n+1}-2^{2n+1}\\&=3^{n+1}(3^n-2^n)+2^{n+1}(3^n-2^n)\\&=(3^n-2^n)(3^{n+1}+2^{n+1}).\end{aligned}$$

当 $n=1$ 时，$3^{2n+1}-2^{2n+1}-6^n=13$ 是素数.

当 $n>1$ 时，由于

$3^n-2^n>1$，$3^{n+1}+2^{n+1}>1$，

所以 $3^{2n+1}-2^{2n+1}-6^n$ 是合数.

因此所求的 n 为 $n\geqslant2$ 的自然数.

例 2 若 a 为自然数，则 a^4-3a^2+9 是素数还是合数？给出你的证明.

解 已知表达式可分解为

$a^4-3a^2+9=(a^2+6a^2+9)-9a^2=(a^2+3a+3)(a^2-3a+3)$.

当 $a=1$ 时，$a^4-3a^2+9=7$ 为素数；

当 $a=2$ 时，$a^4-3a^2+9=13$ 为素数；

当 $a>2$ 时，$a-3\geqslant0$，则

$a^2+3a+3>1$，

$a^2-3a+3=a(a-3)+3>1$.

于是 a^4-3a^2+9 可以分解为两个大于 1 的整数的乘积.

所以，当 $a=1$ 或 2 时，a^4-3a^2+9 为素数.

当 $a>2$ 时，a^4-3a^2+9 是一个合数.

例 3 （IMO - 46 预选题）已知正整数 a、b、c、d、e、f 满足和 $S=a+b+c+d+e+f$ 可以整除 $abc+def$ 与 $ab+bc+ca-de-ef-fd$.

证明：S 是合数.

证明 设 $P(x)=(x+a)(x+b)(x+c)-(x-d)(x-e)(x-f)$

$=Sx^2+(ab+bc+ca-de-ef-fd)x+abc+def$，

则二次多项式 $P(x)$ 的系数都是 S 的倍数. 因此，

$P(d)=(a+d)(b+d)(c+d)$

也是 S 的倍数.

由于 $a+d$、$b+d$、$c+d$ 均小于 S，所以，S 一定是合数.

例 4 （2007 年克罗地亚数学竞赛题）已知方程 $2x^2+mx+2-n=0$ 的两个根均为非零整数. 证明：$\frac{m^2+n^2}{4}$ 是合数.

证明 由韦达定理得

$x_1+x_2=-\frac{m}{2}, x_1x_2=1-\frac{n}{2}$.

则 $m=-2(x_1+x_2), n=2(1-x_1x_2)$.

故 $\frac{m^2+n^2}{4}=(x_1+x_2)^2+(1-x_1x_2)^2$

$=x_1^2+x_2^2+1+x_1^2x_2^2$

$=(x_1^2+1)(x_2^2+1)$.

因为 x_1，x_2 皆为非零整数，所以，$\frac{m^2+n^2}{4}$ 为合数.

例 5 (1986 年第 20 届全苏数学奥林匹克题)方程 $x^2+ax+b+1=0$ 的根是自然数. 证明 a^2+b^2 是合数.

证明 设已知方程的两个根为 x_1, x_2, 则

$x_1+x_2=-a, x_1x_2=b+1.$

于是有

$$\begin{aligned} a^2+b^2 &=(x_1+x_2)^2+(x_1x_2-1)^2 \\ &=x_1^2+x_2^2+2x_1x_2+x_1^2x_2^2-2x_1x_2+1 \\ &=x_1^2x_2^2+x_1^2+x_2^2+1 \\ &=(x_1^2+1)(x_2^2+1). \end{aligned}$$

显然, 由 $x_1\in\mathbf{N}$, $x_2\in\mathbf{N}$ 得 $x_1^2+1>1$, $x_2^2+1>1$.

所以 a^2+b^2 是合数.

例 6 求所有的素数 p, 使 $4p^2+1$ 和 $6p^2+1$ 也是素数.

解 设 $u=4p^2+1$, $v=6p^2+1$,

并设 $p=5k+r$, $k\in\mathbf{Z}, r\in\{0,1,2,3,4\}$.

于是

$u=100k^2+40kr+4r^2+1$,

$u=150k^2+60kr+6r^2+1$.

若 $p\equiv0 \pmod 5$, 则 $u\equiv1$, $v\equiv1 \pmod 5$;

若 $p\equiv1 \pmod 5$, 则 $u\equiv0$, $v\equiv2 \pmod 5$;

若 $p\equiv2 \pmod 5$, 则 $u\equiv2$, $v\equiv0 \pmod 5$;

若 $p\equiv3 \pmod 5$, 则 $u\equiv2$, $v\equiv0 \pmod 5$;

若 $p\equiv4 \pmod 5$, 则 $u\equiv0$, $v\equiv2 \pmod 5$.

因此, 对任何整数 p, 三个数 p, u, v 之中有一个且仅有一个能被 5 整除.

由于当 p 不能被 5 整除时, u 和 v 之中有一个能被 5 整除, 即 u 和 v 之中有一个不是素数, 所以若使 u 和 v 都是素数, 只有 p 能被 5 整除时才有可能. 又由于 p 是素数, 所以 $p=5$.

不难验证, 当 $p=5$ 时, $u=4\cdot5^2+1=101$, $v=6\cdot5^2+1=151$ 都是素数.

因此, 本题只有唯一解.

例 7 (第 20 届爱尔兰数学奥林匹克题)求出所有的素数 p、q 满足

$p\mid(q+6)$ 且 $q\mid(p+7)$.

解 若 $p=2$, 由 $p\mid(q+6)$, 得 $q=2$.

此时, $q\nmid(p+7)$. 故 $p\neq2$.

若 $q=2$, 由 $p\mid(q+6)$, 得 $p=2$.

而 $q\nmid(p+7)$, 矛盾. 故 $q\neq2$.

因此，p、q 均为奇素数.

进而，$p+7$ 为偶数.

因为 $q|(p+7)$，所以，

$$q\leqslant\frac{p+7}{2}\leqslant\frac{q+6+7}{2}.$$

故 $q\leqslant 13$.

用枚举法讨论 $q=3$，5，7，11，13 的情况.

易知当且仅当 $q=13$，$p=19$ 时，满足题意.

例 8 （第 36 届美国数学奥林匹克题）证明：对所有的非负整数 n，$7^{7^n}+1$ 是 $2n+3$ 个素数（不一定互不相同）的乘积.

证明 对 n 用数学归纳法.

当 $n=0$ 时，$7^{7^0}+1=7^1+1=2^3$，结论成立.

假设当 $n=k$ 时，结论成立，即 $7^{7^k}+1$ 至少是 $2k+3$ 个素数的乘积.

当 $n=k+1$ 时，只需证明，对 $m\in\mathbf{N}_+$，记 $x=7^{2m-1}$，$\frac{x^7+1}{x+1}$ 是一个合数［这样，$7^{7^{k+1}}+1$ 至少是 $2k+3+2=2(k+1)+3$ 个素数的乘积］.

注意到，

$$\begin{aligned}\frac{x^7+1}{x+1}&=\frac{(x+1)^7-[(x+1)^7-(x^7+1)]}{x+1}\\&=(x+1)^6-\frac{7x(x^5+3x^4+5x^3+5x^2+3x+1)}{x+1}\\&=(x+1)^6-7x(x^4+2x^3+3x^2+2x+1)\\&=(x+1)^6-7^{2m}(x^2+x+1)^2\\&=[(x+1)^3-7^m(x^2+x+1)]\cdot[(x+1)^3+7^m(x^2+x+1)].\end{aligned}$$

事实上，上式右端的两个因子都大于 1，只需对较小的一个进行检验.

注意到 $\sqrt{7x}\leqslant x$，则

$$\begin{aligned}(x+1)^3-7^m(x^2+x+1)&=(x+1)^3-\sqrt{7x}(x^2+x+1)\\&\geqslant x^3+3x^2+3x+1-x(x^2+x+1)\\&=2x^2+2x+1\geqslant 113>1.\end{aligned}$$

这表明，$\frac{x^7+1}{x+1}$ 是一个合数，结论成立.

例 9 （2002 年澳大利亚国家数学竞赛题）已知多项式 $P(n)=n^3-n^2-5n+2$，求所有整数 n，使得 $P^2(n)$ 是一个素数的平方.

解 设 p 是素数，则 $P^2(n)=p^2$ 成立的充要条件是 $P(n)=\pm p$. 由于

$P(n)=n^3-n^2-5n+2-(n+2)(n^2-3n+1)$，

则要么 $n+2=\pm1$，$n^2-3n+1=\pm p$；

要么 $n^2-3n+1=\pm1$，$n+2=\pm p$.

(1) 当 $n+2=1$ 时，$n^2-3n+1=5$.

(2) 当 $n+2=-1$ 时，$n^2-3n+1=19$.

(3) 当 $n^2-3n+1=1$ 时，

若 $n=0$，$n+2=2$；

若 $n=3$，$n+2=5$.

(4) 当 $n^2-3n+1=-1$ 时，

若 $n=1$，$n+2=3$；

若 $n=2$，$n+2=4$.

因为 4 不是素数，所以，n 的值共 5 个，分别为 -3，-1，0，1，3.

例 10 设 p 是素数，整数 x、y、z 满足 $0<x<y<z<p$. 若 x^3、y^3、z^3 除以 p 的余数相等，证明：$x^2+y^2+z^2$ 可以被 $x+y+z$ 整除.

证明 由已知 $x^3\equiv y^3\equiv z^3 \pmod p$，所以，

$p|(x^3-y^3)$，即 $p|(x-y)(x^2+xy+y^2)$.

又 $0<x<y<p$，p 为素数，故 $p\nmid(x-y)$. 因此，

$p|(x^2+xy+y^2)$. ①

同理可得

$p|(y^2+yz+z^2)$， ②

$p|(x^2+xz+z^2)$. ③

由①、②知，

$p|(x^2+xy+y^2-y^2-yz-z^2)$，即 $p|(x-z)(x+y+z)$.

从而，$p|(x+y+z)$.

已知 $0<x<y<z<p$，所以，

$x+y+z=p$ 或 $2p$.

由于 $p>3$，则 $(2,p)=1$.

又因为 $x+y+z\equiv x^2+y^2+z^2 \pmod 2$，故只须证 $p|(x^2+y^2+z^2)$.

由①得 $p|[x(x+y+z)+y^2-xz]$，于是，

$p|(y^2-xz)$. ④

同理 $p|(x^2-yz)$， ⑤

$p|(z^2-xy)$. ⑥

由①～⑥得 $p|3(x^2+y^2+z^2)$.

故 $p\mid(x^2+y^2+z^2)$.

原题得证.

例 11 （第 55 届捷克和斯洛伐克数学奥林匹克题）求所有的由不同素数组成的三元数组(p,q,r)满足 $p\mid(q+r)$,$q\mid(r+2p)$,$r\mid(p+3q)$.

解 (1) 若 p 是 p，q，r 中最大的素数，由 $p\mid(q+r)$及 $q+r<2p$ 得 $q+r=p$.

由 $q\mid(r+2p)$,得 $q\mid(3r+2q)$,即 $q\mid 3r$.

因为 $q\neq r$,所以,$q=3$.

于是,$p=r+3$.

由 $r\mid(p+3q)$,得 $r\mid(r+12)$,即 $r\mid 12$,所以,

$r=2$，$p=5$.

(2) 若 q 是 p，q，r 中最大的素数，由于 $q\mid(r+2p)$,且 $r+2p<3q$,则

$r+2p=q$ 或 $r+2p=2q$.

若 $2q=r+2p$,则 r 为偶数,从而,$r=2$. 于是,$q=p+1$,矛盾.

若 $q=r+2p$,由 $p\mid(q+r)$,得 $p\mid(2r+2p)$,即 $p\mid 2r$. 因此,$p=2$.

由 $r\mid(p+3q)$,知 $r\mid(3r+7p)$,得 $r\mid(3r+14)$,即 $r\mid 14$,所以,

$r=7$,$q=11$.

(3) 若 r 是 p，q，r 中最大的素数，由于 $r\mid(p+3q)$,且 $p+3q<4r$,则

$p+3q=3r$ 或 $p+3q=2r$ 或 $p+3q=r$.

若 $p+3q=3r$,则 $p=3$. 于是,$r=q+1$,矛盾.

若 $p+3q=2r$,由 $p\mid(q+r)$,得 $p\mid 2(q+r)$,知 $p\mid(p+5q)$,即 $p\mid 5q$. 因此,$p=5$.

由 $q\mid 2(r+2p)$,得 $q\mid(3q+25)$,即 $q\mid 25$,所以,$q=5$,矛盾.

若 $p+3q=r$,由 $p\mid(q+r)$,得 $p\mid(p+4q)$,即 $p\mid 4q$,所以,$p=2$.

由 $q\mid(r+2p)$,得 $q\mid(3q+6)$,即 $q\mid 6$,所以,

$q=3$,$r=p+3q=11$.

综上所述,满足条件的数组共有三组：

$(5,3,2)$,$(2,11,7)$,$(2,3,11)$.

例 12 （2006 年澳大利亚数学奥林匹克题）甲、乙两人玩一个猜数游戏. 甲选一个正整数 a，并告诉乙 $a\leqslant 2006$. 每次乙告诉甲一个正整数 b，则甲告诉乙 $a+b$ 是否是一个素数. 证明：乙问甲的次数小于 2006 就能猜出甲选的数 a.

证明 定义：

数列 $S_n(k)=(k+1,k+2,\cdots,k+n)$，

函数 $f(m)=\begin{cases}1, & m\text{ 为素数},\\0, & m\text{ 为合数},\end{cases}$

$f(S_n(k))=(f(k+1),f(k+2),\cdots,f(k+n))$.

对甲选的正整数 $a(1\leqslant a\leqslant 2006)$，取 b 1，2，…，2005，得到 $f(S_{2005}(a))$.

为确定 a，只须证：对 $1\leqslant i<j\leqslant 2006$，$f(S_{2005}(i))\neq f(S_{2005}(j))$.

下面用反证法.

假设存在 $k\in \mathbf{N}_+$，使得 $1\leqslant i<i+k\leqslant 2006$，且

$f(S_{2005}(i))=f(S_{2005}(i+k))$.

则对任意的 $u\in[i,\ i+2005]$，有

$f(u)=f(u+k)$.

若 $k=1$，显然，2003，2011 之一必在 $[i,\ i+2005]$ 中.

注意到 $f(2003,\ 2011)=(1,1)$，但

$f(2003+1,\ 2011+1)=(0,\ 0)$，

矛盾. 故 $k\neq 1$.

若 $2\nmid k$，显然，2003、2011 之一必在 $[i,\ i+2005]$ 中.

注意到 $f(2003,\ 2011)=(1,1)$，但

$f(2003+k,2011+k)=(0,0)$，矛盾.

故 $2\mid k$.

若 $3\nmid k$，显然，$\{1999,\ 2003\}$、$\{2017,\ 2027\}$ 之一必包含在 $[i,\ i+2005]$ 中，设为 a、b.

注意到 $f(a,\ b)=(1,\ 1)$，但 $0\in f(a+k,\ b+k)$（因 a、b 模 3 余 1、2，故 $a+k$、$b+k$ 之一模 3 余 0），矛盾. 故 $3\mid k$.

若 $5\nmid k$，显然 $\{1871,\ 1873,\ 1877,\ 1879\}$、$\{2003,\ 2011,\ 2017,\ 2029\}$ 之一必包含在 $[i,\ i+2005]$ 中，设为 a、b、c、d.

注意到 $f(a,b,c,d)=(1,1,1,1)$，但 $0\in f(a+k,b+k,c+k,d+k)$（因 a、b、c、d 模 5 余 1、2、3、4，则 $a+k$、$b+k$、$c+k$、$d+k$ 之一模 5 余 0），矛盾. 故 $5\mid k$.

从而，$30\mid k$.

于是，$k\geqslant 30$，$i\leqslant 2006-k\leqslant 2006-30=1976$.

若 $7\nmid k$，显然，$\{1987,1993,1997,1999,2003\}\subset[i,i+2005]$，且 1949、2089 之一必在 $[i,i+2005]$ 中，设为 a、b、c、d、e、g，其模 7 分别余 1、2、3、4、5、6.

注意到 $f(a,b,c,d,e,g)=(1,1,1,1,1,1)$，但 $0\in f(a+k,b+k,c+k,d+k,e+k,g+k)$，矛盾. 故 $7\mid k$.

从而，$210\mid k$.

于是，$k\geqslant 210$，$i\leqslant 2006-k\leqslant 2006-210=1796$.

若 $11\nmid k$，显然，$\{1831,1873,1879,1973,1979,1987,1993,1997,1999,2003\}\subseteq$

$[i,i+2005]$，设为 a_1，a_2，…，a_{10}，其模 11 分别余 1，2，…，10.

注意到 $f(a_1,a_2,\cdots,a_{10})=(1,1,\cdots,1)$，但 $0\in f(a_1+k,a_2+k,\cdots,a_{10}+k)$，矛盾. 故 $11|k$.

从而，$2310|k$.

于是，$k\geqslant 2310$，与 $k\leqslant 2005$ 矛盾.

因此，所证命题成立.

【解题思维策略分析】

1. 仔细分析条件，求解满足某些条件的素数

例 13 （第 25 届巴西数学奥林匹克题）求最小的正素数，使得对于某个整数 n，这个素数能整除 $n^2+5n+23$.

解 设 $f(n)=n^2+5n+23$. 因为

$f(n)\equiv 1(\bmod 2)$，$f(n)\equiv\pm 1(\bmod 3)$，

$f(n)\equiv -1,\pm 2(\bmod 5)$，

$f(n)\equiv 1,3,\pm 2(\bmod 7)$，

$f(n)\equiv 1,\pm 3,\pm 4,6(\bmod 11)$，

$f(n)\equiv -2,\pm 3,4,-5,\pm 6(\bmod 13)$，

且 $f(-2)=17$，

所以，满足条件的最小的正素数为 17.

例 14 （2004 年丝绸之路数学竞赛题）求所有的素数 p，使得存在整数 m，n 满足 $p=m^2+n^2$，且 $p|(m^3+n^3-4)$.

解 当 $|m|$、$|n|\leqslant 3$ 时，素数 $2=1^2+1^2$，$5=1^2+2^2$，$13=(-3)^2+(-2)^2$ 满足条件.

下面证明，仅有这些素数满足条件.

由 $p=m^2+n^2$，得 $mn=\dfrac{(m+n)^2-p}{2}$，于是，有

$$m^3+n^3-4=(m+n)^3-3(m+n)mn-4=\frac{-(m+n)^3+3p(m+n)-8}{2}.$$

由 $p|(m^3+n^3-4)$，有 $p|[(m+n)^3+8]$.

于是，要么 $p|(m+n+2)$；要么 $p|[(m+n)^2-2(m+n)+4]$，即当 $p>2$ 时，等价于 $p|(mn-m-n+2)$.

(1) $p|(m+n+2)$.

注意到 $m^2+n^2\leqslant|m+n+2|$.

当 $m^2+n^2\leqslant m+n+2$ 时，有

$(2m-1)^2+(2n-1)^2\leqslant 10$，可得 $-1\leqslant m$，$n\leqslant 2$；

当 $m^2+n^2\leqslant -(m+n+2)$ 时，有

$(2m+1)^2+(2n+1)^2\leqslant -6$，无解.

(2) $p\mid(mn-m-n+2)$.

注意到 $m^2+n^2\leqslant|mn-m-n+2|$.

当 $m^2+n^2\leqslant mn-m-n+2$ 时，有

$(2m-n+1)^2+3(n+1)^2\leqslant 12$，可得 $-3\leqslant m$，$n\leqslant 1$；

当 $m^2+n^2\leqslant -(mn-m-n+2)$ 时，有

$(2m+n-1)^2+3\left(n-\frac{1}{3}\right)^2\leqslant -\frac{20}{3}$，无解.

例 15 （第 29 届俄罗斯数学奥林匹克题）求所有素数 p，使得 $p^x=y^3+1$ 成立，其中 x，y 是正整数.

解 因为 $p^x=(y+1)(y^2-y+1)$，$y>0$，所以，$y+1\geqslant 2$.

令 $y+1=p^t$（$t\in\mathbf{Z}_+$，$1\leqslant t\leqslant x$），则

$y=p^t-1$.

从而，$y^2-y+1=p^{x-t}$.

将 $y=p^t-1$ 代入得

$(p^t-1)^2-(p^t-1)+1=p^{x-t}$，即 $p^{2t}-3p^t+3=p^{x-t}$.

故 $p^{x-t}(p^{3t-x}-1)=3(p^t-1)$.

(1) 当 $p=2$ 时，$p^{3t-x}-1$，p^t-1 为奇数，则 p^{x-t} 为奇数.

故 $x=t$，$y^2-y+1=1$.

因此，$y=1$，$p=2$，$x=1$.

(2) 当 $p\neq 2$ 时，p 为奇数，则 $p^{3t-x}-1$，p^t-1 为偶数，p^{x-t} 为奇数.

从而，$3\mid p^{x-t}$ 或 $3\mid(p^{3t-x}-1)$.

当 $3\mid p^{x-t}$ 时，$p=3$，$x=t+1$，则

$y^2-y+1=3$.

解得 $y=2$，$x=2$.

当 $3\mid(p^{3t-x}-1)$ 时，有 $p^{x-t}\mid(p^t-1)$，$x=t$.

由 (1) 得 $y=1$，$p=2$. 矛盾.

综上所述，有两组解

$p=2$，$x=1$，$y=1$ 和 $p=3$，$x=2$，$y=2$.

例 16 （1999 年国家集训队选拔考试题）试求满足以下条件的全部素数 p：对任一素数 $q<p$，若 $p=kq+r$，$0\leqslant r<q$，则不存在大于 1 的整数 a，使得 a^2 整除 r.

解 注意到 $p=2$，$p-3=1\times2+1$，

$p=5=2\times2+1=1\times3+2$，$p=7=2\times3+1=1\times5+2$.

均满足题目要求的条件.

而 $p=11=1\times7+4=1\times7+2^2$，

$p=11$ 不满足题目要求条件.

现考虑 $p>11$ 的情形.

考察 $p-r=kq$，$0\leqslant r<q$. ①

显然，由素数 $q<$ 素数 p，及 $p>11$ 知

$r\neq1$，2，3，5，6，7，10，11，12.

现研究 $p-4$，$p-8$，$p-9$.

由于 $p-4$ 不能含有大于 3 的素约数，由①

$p-4=3^a$，$a\geqslant2$.

由于 p 是奇素数，所以 $p-9$ 是偶数，含有素约数 2，且它的素约数不超过 7.

由于 $p-9=3^a-5$，则 $p-9$ 不能含素约数 5.

于是，$p-9$ 只能含素约数 2 和 7.

再考虑 $p-9$ 所含素约数 2 的最高次幂.

$$p-9=3^a-5\equiv\begin{cases}1-5\\3-5\end{cases}\equiv\begin{cases}4\\6\end{cases}\pmod 8,$$

于是 $8\nmid p-9$.

这样，$p-9$ 只有两种可能：

$p-q=2\cdot7^b$，或 $p-9=2^2\cdot7^b$.

若 $p-9=2\cdot7^b$，则 $3^a-5=2\cdot7^b$，即 $3^a=2(7^b+1)+3$.

由此得 $0\equiv7\equiv1\pmod 3$，矛盾.

于是只有 $p-9=4\cdot7^b$， ②

或 $p-8=4\cdot7^b+1$.

由于 $p-8$ 不含大于 7 的素约数.

由 $3\mid p-4$ 得 $3\nmid p-8$.

由 $7\mid p-9$ 得 $7\nmid p-8$.

这样，$p-8$ 只含素约数 5，

$p-8=5^c$. ③

于是，由②和③得 $4\cdot7^b=5^c-1$，$b\geqslant0$，$c\geqslant1$.

若 $b\geqslant1$，考察数列

$\{5^c-1\pmod 7\}=\{4,3,5,1,2,0,4,3,5,1,2,0,\cdots\}$，

于是 c 是 6 的倍数.

设 $c=2c'$, $c'\geqslant1$, 则

$4\cdot7^b=25^{c'}-1$, 即 $24|4\cdot7^b$, 这是不可能的.

所以, $b\geqslant1$ 不成立.

于是 $b=0$, $c=1$, 故

$p-8=4\cdot7^0+1$, 即 $p=13$.

综上, $p=2, 3, 5, 7, 13$.

例 17 (IMO-28 试题) 已知 $n\geqslant2$, 且对 $0\leqslant k\leqslant\sqrt{\frac{n}{3}}$, k^2+k+n 是素数, 求证对 $0\leqslant k\leqslant n-2$, k^2+k+n 也是素数.

证法 1 假设对所有的 k, $0\leqslant k\leqslant n-2$, k^2+k+n 不都是素数, 即存在一些 k, $0\leqslant k\leqslant n-2$, 使得 k^2+k+n 是合数.

设 k_0 是使得 k^2+k+n 是合数的最小的 k, 则 $k_0\leqslant n-2$, $k_0^2+k_0+n$ 是合数.

再设 q 是 $k_0^2+k_0+n$ 的最小素因子, 则 $q^2\leqslant k_0^2+k_0+n$.

我们首先证明 $q>2k_0$.

若 $q\leqslant2k_0$, 考虑差

$(k_0^2+k_0+n)-(k^2+k+n)=(k_0-k)(k_0+k+1)$.

取 $k=0, 1, 2, \cdots, k_0-1$, 则由 k_0 的规定, k^2+k+n 为素数.

此时, $k_0-k=1, 2, \cdots, k_0$, $k_0+k+1=k_0+1, k_0+2, \cdots, 2k_0$.

于是 k_0-k 与 k_0+k+1 遍取 $1, 2, \cdots, 2k_0$ 诸数, 由于 $q\leqslant2k_0$, 则存在一个 k, 使得

$$q|(k_0-k)(k_0+k+1).\qquad①$$

又因为 $q|k_0^2+k_0+n$, 则 $q|k^2+k+n$.

鉴于 k^2+k+n 是素数, 则有 $q=k^2+k+n$.

由于 $k_0-k\leqslant k_0\leqslant n-2<n+k+k^2=q$,

$k_0+k+1\leqslant(n-2)+k+1=n+k-1<n+k+k^2=q$,

所以

$$q\nmid(k_0-k)(k_0+k+1).\qquad②$$

①与②矛盾.

因此, $q>2k_0$, 即 $q\geqslant2k_0+1$.

由于 $k_0^2+k_0+n\geqslant q^2\geqslant(2k_0+1)^2=4k_0^2+4k_0+1$, 即

$3k_0^2\leqslant n-1-3k_0\leqslant n-1<n$,

$k_0<\sqrt{\frac{n}{3}}$.

由已知条件，当 $k_0<\sqrt{\frac{n}{3}}$ 时，$k_0^2+k_0+n$ 是素数，与 $k_0^2+k_0+n$ 为合数矛盾.

因此，这样的 k_0 不存在，即对 $k=0, 1, 2, \cdots, n-2$，k^2+k+n 都是素数.

证法 2 假设存在一些 k，$0\leqslant k\leqslant n-2$，使得 k^2+k+n 不是素数，由 $n\geqslant 2$，则 k^2+k+n 为合数.

设 k_0 是使得 k^2+k+n 为合数的最小的 k，即 $k_0^2+k_0+n$ 为其中的最小的合数.

又设 q 是 $k_0^2+k_0+n$ 的最小素因子.

(1) 若 $q\leqslant k_0$，则可设 $k_0=q+b(b\geqslant 0)$. 于是

$$\begin{aligned}k_0^2+k_0+n&=(q+b)^2+(q+b)+n\\&=q(q+2b+1)+(b^2+b+n).\end{aligned}$$

由于 $b<k_0$，则

$b^2+b+n<k_0^2+k_0+n$，

由 k_0 的假设，b^2+b+n 是素数.

又由于 $q\mid k_0^2+k_0+n$，$q\mid q(q+2b+1)$，则

$q\mid b^2+b+n$，

所以必有 $q=b^2+b+n$.

此时有 $q=b^2+b+n>n-2$，而 $q\leqslant k_0<n-2$，出现矛盾.

(2) 若 $q>k_0$，则可设 $q=k_0+b$，于是

$$\begin{aligned}k_0^2+k_0+n&=(q-b)^2+(q-b)+n\\&=q(q-2b+1)+(b-1)^2+(b-1)+n.\end{aligned}$$

当 $b-1<k_0$ 时，

由 $b-1<k_0\leqslant n-2$，可知 $(b-1)^2+(b-1)+n$ 是素数.

所以有 $(b-1)^2+(b-1)+n=q$.

于是 $q^2\leqslant k_0^2+k_0+n=q(q-2b+1)+q=q^2-2bq+2q$，

从而 $b\leqslant 1$.

于是只能有 $b=1$，即 $q=n$ 是素数.

又由 $q=k_0+b=k_0+1=n$，而 $k_0+1\leqslant n-2+1=n-1$，

于是 $n\leqslant n-1$.

导致矛盾.

因此只能有 $b-1\geqslant k_0$，即

$b\geqslant k_0+1$.

$q-k_0+b\geqslant 2k_0+1$.

于是 $(2k_0+1)^2\leqslant q^2\leqslant k_0^2+k_0+n$，

$4k_0^2+4k_0+1\leqslant k_0^2+k_0+n$,

$n\geqslant 3k_0^2+3k_0+1>3k_0^2$,

$k_0<\sqrt{\frac{n}{3}}$.

然而由已知，当 $k_0<\sqrt{\frac{n}{3}}$ 时，$k_0^2+k_0+n$ 是素数，与 $k_0^2+k_0+n$ 是合数矛盾.

由以上知，当 $0\leqslant k_0\leqslant n-2$ 时，$k_0^2+k_0+n$ 都是素数，从而命题得证.

2. 合数的证明

例 18 （1984 年第 10 届全俄数学奥林匹克题）自然数 a，b，c，d 满足等式 $ab=cd$. 求证 $k=a^{1984}+b^{1984}+c^{1984}+d^{1984}$ 是合数.

证明 由 $ab=cd$，可设

$a=uv$，$b=wt$，$c=uw$，$d=vt$，其中 u，v，w，t 是自然数，

于是

$$\begin{aligned}k&=a^{1984}+b^{1984}+c^{1984}+d^{1984}\\&=(uv)^{1984}+(wt)^{1984}+(uw)^{1984}+(vt)^{1984}\\&=u^{1984}(v^{1984}+w^{1984})+t^{1984}(w^{1984}+v^{1984})\\&=(u^{1984}+t^{1984})(v^{1984}+w^{1984}).\end{aligned}$$

由于 u，v，w，t 是自然数，则

$u^{1984}+t^{1984}>1$，$v^{1984}+w^{1984}>1$.

于是 k 是合数.

例 19 （1991 年列宁格勒数学奥林匹克题）证明数 $512^3+675^3+720^3$ 是合数.

证明 令 $x=512$，$y=675$，$z=720$，则

$x=2^9$，$y=3^3\cdot 5^2$，$z=2^4\cdot 3^2\cdot 5$.

于是 $2z^2=3xy$.

从而有

$$\begin{aligned}x^3+y^3+z^3&=x^3+y^3-z^3+2z^2\cdot z\\&=x^3+y^3-z^3+3xyz\\&=x^3+y^3-z^3-3xy(-z)\\&=(x+y-z)(x^2+y^2+z^2-xy+xz+yz).\end{aligned}$$

由 $x+y-z>1$，$x^2+y^2+z^2-xy+xz+yz>1$，可知 $x^3+y^3+z^3=512^3+675^3+720^3$ 是合数.

例 20 （1985 年第 11 届全俄数学奥林匹克题）证明 $1010\cdots101$（含 k 个 0 及 $k+1$ 个 1，$k\geqslant 2$）为合数.

证明 设此数为 x_k，则

$$x_k=1010\cdots101=100^k+100^{k-1}+\cdots+100+1$$
$$=\frac{100^{k+1}-1}{100-1}=\frac{(10^{k+1})^2-1}{99}$$
$$=\frac{(10^{k+1}+1)(10^{k+1}-1)}{99}.$$

(1) 若 k 为偶数，则 $k+1$ 为奇数，于是

$10+1=11\mid 10^{k+1}+1, 10-1=9\mid 10^{k+1}-1.$

从而 $x_k=\dfrac{10^{k+1}+1}{11}\cdot\dfrac{10^{k+1}-1}{9}.$

上式是两个大于 1 的整数之积，因而 x_k 是合数.

(2) 若 k 为奇数，则 $k+1$ 为偶数. 设 $k+1=2t$，其中 $t\geqslant2$，$t\in\mathbf{N}$，于是

$$x_k=\frac{10^{k+1}-1}{99}\cdot(10^{k+1}+1)=\frac{100^t-1}{99}(10^{k+1}+1).$$

因为 $100-1=99\mid 100^t-1$，且 $\dfrac{100^t-1}{99}>1$（因为 $t\geqslant2$），$10^{k+1}+1>1$，所以 x_k 是两个大于 1 的整数之积，因而 x_k 是合数.

例 21 （IMO－32 预选题）证明 $N=\dfrac{5^{125}-1}{5^{25}-1}$ 不是素数.

证明 令 $x=5^{25}$，则

$$N=\frac{x^5-1}{x-1}=x^4+x^3+x^2+x+1$$
$$=(x^2+3x+1)^2-5x(x+1)^2=(x^2+3x+1)^2-5^{26}(x+1)^2$$
$$=[(x^2+3x+1)+5^{13}(x+1)][(x^2+3x+1)-5^{13}(x+1)].$$

显然，$(x^2+3x+1)+5^{13}(x+1)>1$，

$(x^2+3x+1)-5^{13}(x+1)>1$，

于是 N 是两个大于 1 的自然数的乘积，不可能是素数.

例 22 （1990 年国家集训队测验题）若 x_0，a，$b\in\mathbf{N}$，$x_{n+1}=x_na+b(n=0,1,2,\cdots)$. 证明 x_n 不可能全为素数.

证明 (1) 若 $(a,b)=d>1$，则 $d\mid x_1=x_0a+b$.

即 x_1 是合数.

(2) 若 $(a,b)=1$，则 $(x_1,a)=(a,b)=1$.

在 x_1，x_2，x_3，…中，至少有两个数关于 $\bmod x_1$ 同余，设这两个数为 x_k，x_{k+T} $(T\geqslant1)$，则

$x_k\equiv x_{k+T}\pmod{x_1}$，

$ax_{k-1}+b\equiv ax_{k+T-1}+b \pmod{x_1}$,

$ax_{k-1}\equiv ax_{k+T-1} \pmod{x_1}$.

又因为$(x_1,a)=1$，则 $x_{k-1}\equiv x_{k+T-1} \pmod{x_1}$.

从而有 $x_1\equiv x_{1+T} \pmod{x_1}$，即 $x_1 \mid x_{1+T}$.

而 $x_{1+T}\geqslant x_2>x_1$，又有 $x_1=ax_0+b>1$，于是

$x_{1+T}>1$.

故 x_{1+T}为合数.

3. 抓住素数条件，求解其他问题

例 23 （1993 年韩国数学奥林匹克题）求所有非负整数 n，使得 $2^{2^n}+5$ 是一个素数.

解 当 $n=0$ 时，

$2^{2^n}+5=2^{2^0}+5=2^1+5=2+5=7$ 是素数.

当 $n>1$ 时，因为 $2\equiv-1 \pmod 3$，所以

$2^{2^n}+5\equiv(-1)^{2^n}+2=1+2\equiv 0 \pmod 3$，且 $2^{2^n}+5>3$，

从而 $2^{2^n}+5$ 是 3 的倍数，且不等于 3，故它必是合数.

综上所述，所求的非负整数仅有 $n=0$.

例 24 （1989 年第 50 届美国普特南数学竞赛题）设 K 是这样的自然数的全体，其中每一个数由 0 与 1 两个数字相间而成，首位与末位都是 1，问 K 中有多少个素数?

解 1 不是素数，而 101 是素数.

设 101010…01 中有 3 个或 3 个以上的 1.

这种数总可以表示为

$$1+100+100^2+\cdots+100^n=\frac{100^{n+1}-1}{100-1}(n\geqslant 2).$$

由于

$$\frac{100^{n+1}-1}{100-1}=\frac{10^{2n+2}-1}{10^2-1}=\frac{(10^{n+1}+1)(10^{n+1}-1)}{(10+1)(10-1)}$$

$$=\frac{(10^{n+1}+1)\cdot 99\cdots9}{(10+1)\cdot 9}=\frac{(10^{n+1}+1)}{(10+1)}\cdot 11\cdots1.$$

如果 n 为奇数，那么 $n+1$ 为偶数，这时$\frac{11\cdots11}{11}$是大于 1 的整数.

从而$\frac{11\cdots11}{11}\cdot(10^{n+1}+1)$是两个大于 1 的整数的乘积，即$\frac{100^{n+1}-1}{100-1}$是合数.

如果 n 为偶数，那么 $n+1$ 为奇数，这时 $10+1$ 能整除 $10^{n+1}+1$，并且商大于 1.

从而$\frac{10^{n+1}+1}{10+1}\cdot 11\cdots11$ 是两个大于 1 的整数的乘积，即$\frac{100^{n+1}-1}{100-1}$是合数.

这就表明，当 $n\geqslant 2$ 时，这种数总是合数.

因此，K 中的素数只有一个，即 101.

例 25 （2007 年保加利亚国家队选拔赛题）求所有的正整数 x，y，使得 $(x^2+y)(y^2+x)$ 是一个素数的 5 次幂.

解 设 $(x^2+y)(y^2+x)=p^5$，其中，p 为素数，则

$x^2+y=p^s$，$y^2+x=p^t$，其中，$\{s,t\}=\{1,4\}$ 或 $\{2,3\}$.

在第一种情况，不妨假设 $x<y$，则

$x^2+y=p$，$y^2+x=p^4$，故

$p^2=(x^2+y)^2>x+y^2=p^4$，矛盾.

于是，设 $x<y$，$x^2+y=p^2$，$y^2+x=p^3$，且 $x<p$.

因为 $p^2\mid[(x^2+y)(x^2-y)+(y^2+x)]=x^4+x=x(x+1)(x^2-x+1)$，所以，

$p^2\mid(x+1)(x^2-x+1)$.

若 p $(x+1)$，则 $p=x+1$，于是，

$(x+1)\mid(x^2-x+1)=(x+1)(x-2)+3$.

从而，$x=2$，$p=3$，$y=5$.

若 $p\nmid(x+1)$，则 $p^2\mid(x^2-x+1)$.

因为 $p^2\mid(x^2+y)=(x^2-x+1)+(x+y-1)$，

所以 $p^2\mid(x+y-1)$.

于是，$y\geqslant p^2-x+1>p^2-p$，$p^3=y^2+x>p^2(p-1)^2$. 矛盾.

综上所述，解为 (2，5) 和 (5，2).

例 26 （第 18 届韩国数学奥林匹克题）设 p 是一个素数，且

$f_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$.

(1) 对任何一个能被 p 整除的整数 m，是否存在一个素数 q，使得 q 整除 $f_p(m)$，且 q 与 $m(m-1)$ 互素？

(2) 证明：存在无限多个正整数 n，使得 $pn+1$ 是素数.

解 (1) 设 q 是任何一个能整除 $f_p(m)$ 的素数. 由于 $f_p(m)\equiv 1(\bmod m)$，故 $(m,q)=1$.

如果 $m\equiv 1(\bmod q)$，则 $f_p(m)\equiv p(\bmod q)$，有 $q\mid p$. 但将导致矛盾（因为 m 可以被 p 整除），所以，$f_p(m)$ 的任一个素因子都满足条件.

(2) 用反证法.

设 p_1，p_2，…，p_N 是仅有的 N 个具有形式 $pn+1$ 的素数. 令 $m=p_1p_2\cdots p_Np$，而 q 是任何一个能整除 $f_p(m)$ 的素数，由 (1) 知，$m\not\equiv 0$，$1(\bmod q)$. 由欧拉定理可知 $m^{q-1}=1(\bmod q)$，及 $m^p=1(\bmod q)$. 由此容易证明 $q-1$ 能被 p 整除，矛盾. 因此，

所证结论成立.

例 27 （2005 年西部数学奥林匹克题）设 $S=\{1,2,\cdots,2005\}$，若 S 中任意 n 个两两互素的数组成的集合中都至少有一个素数，试求 n 的最小值.

解 首先，我们有 $n\geqslant16$. 事实上，取集合

$A_0=\{1,2^2,3^2,5^2,\cdots,41^2,43^2\}$，

其元素，除 1 以外，均为不超过 43 的素数的平方，则 $A_0\subseteq S$，$|A_0|=15$，A_0 中任意两数互素，但其中无素数，这表明 $n\geqslant16$.

其次，我们证明：对任意 $A\subseteq S$，$n=|A|=16$，A 中任两数互素，则 A 中必存在一个素数.

利用反证法，假设 A 中无素数. 记 $A=\{a_1,a_2,\cdots,a_{16}\}$，分两种情况讨论.

(1) 若 $1\notin A$，则 a_1，a_2，…，a_{16} 均为合数，又因为 $(a_i,a_j)=1(1\leqslant i<j\leqslant16)$，所以 a_i 与 a_j 的素因数均不相同，设 a_i 的最小素因数为 p_i，不妨设 $p_1<p_2<\cdots<p_{16}$，则

$a_1\geqslant p_1^2\geqslant2^2$，$a_2\geqslant p_2^2\geqslant3^2$，…，$a_{15}\geqslant p_{15}^2\geqslant47^2>2005$，

矛盾.

(2) 若 $1\in A$，则不妨设 $a_{16}=1$，a_1，…，a_{15} 均为合数，同 (1) 所设，同理有 $a_1\geqslant p_1^2\geqslant2^2$，$a_2\geqslant p_2^2\geqslant3^2$，…，$a_{15}\geqslant p_{15}^2\geqslant47^2>2005$，矛盾.

由 (1)，(2) 知，反设不成立，从而 A 中必有素数，即 $n=|A|=16$ 时结论成立.

综上所述，所求的 n 最小值为 16.

例 28 （1994 年国家集训队选拔考试题）p，q 是两个不同的素数，正整数 $n\geqslant3$. 求所有整数 a，使得多项式 $f(x)=x^n+ax^{n-1}+pq$ 能够分解为两个不低于一次的整系数多项式的积.

解 设 $f(x)=x^n+ax^{n-1}+pq=g(x)h(x)$. ①

可设 $g(x)$，$h(x)$ 的最高次项的系数为 $+1$，否则可考虑 $(-g(x))\cdot(-h(x))$. 即设

$g(x)=x^l+a_{l-1}x^{l-1}+\cdots+a_1x+a_0$， ②

$h(x)=x^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$. ③

显然 $a_0b_0=pq$. ④

由 p，q 是不同的素数及④式，可设 $p\nmid a_0$，则 $p\mid b_0$.

设 $p\mid b_k(k=0,1,\cdots,r-1)$，$p\nmid b_r(r\leqslant m)$，

记 $f(x)$ 中 x^r 的系数为 c_r，则由①，②及③有

$c_r=a_0b_r+a_1b_{r-1}+\cdots+a_rb_0$.

由 $p\nmid a_0$ 知 $p\nmid c_r$，又由题设条件 $c_1=c_2=\cdots=c_{n-2}=0$，它们全是 p 的倍数.

由于 $r\leqslant m\leqslant n-1$，所以只可能是 $r=n-1$，即

$h(x)$为 $n-1$ 次多项式，$g(x)$为一次多项式，$g(x)=x+a_0$.

从而 $f(-a_0)=0$，即 $0=(-a_0)^n+a(-a_0)^{n-1}+pq$，则

$$(-a_0)^{n-1}(a-a_0)=-pq. \quad ⑤$$

由 $n-1\geqslant 2$ 及 p，q 是不同素数，则由上式知 $a_0=\pm 1$.

此时由⑤式有 $a=1+(-1)^n pq$ 或 $a=-1-pq$.

例 29 （1984 年第 18 届全苏数学奥林匹克题）如果一个自然数是素数，而且把它的各位数码经过任意交换后仍然是素数，则称这个素数为绝对素数.

证明绝对素数不能有多于 3 个不同的数字.

证明 绝对素数的各位数码都应是奇数，而且不可能有数码 5. 假设某个绝对素数含有四个不同的数码 1，3，7，9，则可设

$M_1=\overline{a_1a_2\cdots a_n1379}$，并令 $M=\overline{a_1a_2\cdots a_n}$，$a_i\in\{1,3,7,9\}$，$1\leqslant i\leqslant n$.

$M_1=M\cdot 10^4+1379, 1379\equiv 0 \pmod 7$,

$M_2=M\cdot 10^4+1397, 1397\equiv 4 \pmod 7$,

$M_3=M\cdot 10^4+1973, 1973\equiv 6 \pmod 7$,

$M_4=M\cdot 10^4+1937, 1937\equiv 5 \pmod 7$,

$M_5=M\cdot 10^4+1739, 1739\equiv 3 \pmod 7$,

$M_6=M\cdot 10^4+3197, 3197\equiv 5 \pmod 7$,

$M_7=M\cdot 10^4+3179, 3179\equiv 1 \pmod 7$,

$M_8=M\cdot 10^4+9137, 9137\equiv 2 \pmod 7$,

$M_9=M\cdot 10^4+7913, 7913\equiv 3 \pmod 7$.

这九个数被 7 除的余数不同，因此在 M_1，M_2，…，M_9 中一定有一个能被 7 整除而不是素数，从而出现矛盾.

所以绝对素数不可能有多于 3 个不同的数码.

例 30 （1995 年国家集训队选拔考试题）求不能表示成$|3^a-2^b|$的最小素数 p，这里 a 和 b 是非负整数.

解 经检验，2，3，5，7，11，13，17，19，23，29，31，37 都可以写成$|3^a-2^b|$的形式，其中 a，b 是非负整数：

$2=3^1-2^0$，$3=2^2-3^0$，$5=2^3-3^1$，

$7=2^3-3^0$，$11=3^3-2^4$，$13=2^4-3^1$，

$17=3^4-2^6$，$19=3^3-2^3$，$23=3^3-2^2$，

$29=2^5-3^1$，$31=2^5-3^0$，$37=2^6-3^3$.

猜测 41 是不能表示成这种形式的最小素数．为了证实这一猜测，我们用反证法.

如果方程

$$2^u-3^v=41 \tag{①}$$

有非负整数解 (u, v)，则有

$2^u>41$，即 $u\geqslant 6$.

因此，$3^v\equiv -1 \pmod 8$，但 3^v 模 8 的剩余只可能是 1 或 3，矛盾．故方程①无非负整数解.

如果方程

$$3^x-2^y=41 \tag{②}$$

有非负整数解(x,y)，则

$3^x>41$，即 $x\geqslant 4$.

因此 $2^y\equiv 1 \pmod 3$，从而 y 是偶数．设 $y=2t$，则②化为

$3^x-4^t=41$.

于是，我们有

$3^x\equiv 1 \pmod 4$.

从而 x 也是偶数．设 $x=2s$，则②化为

$3^{2s}-2^{2t}=41$，即$(3^s+2^t)(3^s-2^t)=41$.

因此 41 是素数，所以有

$$\begin{cases}3^s+2^t=41,\\ 3^s-2^t=1,\end{cases} \text{即} \begin{cases}3^s=21,\\ 2^t=20.\end{cases}$$

这是不可能的．故方程②没有非负整数解.

综上所述，41 不能表示成$|3^a-2^b|$的形式，其中 a 和 b 是非负整数.

故所求的最小素数 p 为 41.

例 31 （2003 年越南国家队选拔赛题）设 n 是正整数，求证：2^n+1 不存在模 8 余-1的素因子.

证明 对素数 $p\equiv -1 \pmod 8$，考虑

$$2, 2\times 2, 2\times 3, 2\times 4, \cdots, 2\times\frac{p-1}{2}.$$

记其中不大于$\frac{p-1}{2}$的数为 r_1，r_2，…，r_h，大于$\frac{p-1}{2}$的数为 s_1，s_2，…，s_g. 易知

$r_i=r_j\Leftrightarrow i=j(1\leqslant i,j\leqslant h)$，

$s_i - s_j \Leftrightarrow i=j(1\leqslant i,j\leqslant g)$.

若 $p-s_i=r_j$，则 $2|p$. 矛盾.

所以，$p-s_i\neq r_j$(任意的 $1\leqslant i\leqslant g, 1\leqslant j\leqslant h$).

因为 $p-s_i\leqslant\frac{p-1}{2}(1\leqslant i\leqslant g)$，则

$$r_1r_2\cdots r_h(p-s_1)(p-s_2)\cdots(p-s_g)=\left(\frac{p-1}{2}\right)!.$$

故 $r_1r_2\cdots r_h(s_1s_2\cdots s_g)\equiv(-1)^g\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\ p)$.

所以，$2^{\frac{p-1}{2}}\times\left(\frac{p-1}{2}\right)!\equiv(-1)^g\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\ p)$.

从而，$2^{\frac{p-1}{2}}\equiv(-1)^g(\mathrm{mod}\ p)$.

又因为 $2\times\frac{p-3}{4}<\frac{p-1}{2}$，$2\times\frac{p+1}{4}>\frac{p-1}{2}$，所以，$g=\frac{p+1}{4}$.

设 $p=8k-1$，则

$2^{4k-1}\equiv1(\mathrm{mod}\ p)$.

(以上是复述 Gauss 引理)

设 n_0 为最小的正整数，使得 $2^{n_0}\equiv1(\mathrm{mod}\ p)$，则 $n_0|(4k-1)$(由 $4k-1=n_0a+b$，$0\leqslant b<n_0$，有 $2^b\equiv1(\mathrm{mod}\ p)\Rightarrow b=0$).

若存在 n，使得 $2^n\equiv-1(\mathrm{mod}\ p)$. 取其中最小的正整数 n_1，易知 $n_1<n_0$[否则，$2^{n_1-n_0}\equiv2^{n_1-n_0}\times2^{n_0}=2^{n_1}\equiv-1(\mathrm{mod}\ p)$，与 n_1 的最小性矛盾].

设 $n_0=n_1c+d$，$0\leqslant d<n_1$，则

$1\equiv2^{n_0}=2^{n_1c}\times2^d\equiv(-1)^c2^d(\mathrm{mod}\ p)$.

若 c 为奇数，则 $2^d\equiv-1\ (\mathrm{mod}\ p)$，与 n_1 的最小性矛盾.

所以，c 为偶数，且 $d=0$，即 $n_0=2en_1$. 与 $n_0|(4k-1)$矛盾.

因此，不存在 n，使得 2^n+1 有模 8 余-1的素因子.

例 32 (1992 年国家集训队选拔考试题) 任给素数 p. 试证存在整数 x_0，使得 $p|(x_0^2-x_0+3)$的充分必要条件为存在整数 y_0，使得 $p|(y_0^2-y_0+25)$.

证法 1 易知 $x_0^2-x_0+3$ 和 $y_0^2-y_0+25$ 都是奇数，从而不妨设 p 为奇素数. 于是

$p|(x_0^2-x_0+3)\Leftrightarrow p|4(x_0^2-x_0+3)\Leftrightarrow p|(2x_0-1)^2+11$，

$p|(y_0^2-y_0+25)\Leftrightarrow p|4(y_0^2-y_0+25)\Leftrightarrow p|(2y_0-1)^2+3^2\cdot11$.

于是只须证明：存在 x_0，使得 $p|(2x_0-1)^2+11$ 的充要条件是存在 y_0，使得 $p|(2y_0-1)^2+3^2\cdot11$.

(1) 若存在 x_0 使 $p|(2x_0-1)^2+11$,则

$p|3^2(2x_0-1)^2+3^2\cdot 11$,即 $p|[2(3x_0-1)-1]^2+3^2\cdot 11$.

只须取 $y_0=3x_0-1$,就有 $p|(2y_0-1)^2+3^2\cdot 11$.

(2) 若存在 y_0,使得 $p|(2y_0-1)^2+3^2\cdot 11$.

当 $p=3$ 时,只须取 $x_0=1$,即有

$p|(2\cdot 1-1)^2+11=12$.

当 $p>3$ 时,因为$(p,3)=1$,所以存在整数 a 和 b,使得

$ap+3b=1$.

由此对任意整数 k,有

$(a-3k)p+3(b+pk)=1$.

所以存在 a_1 和 b_1,使得

$$a_1p+3b_1=1, \tag{①}$$

且 b_1 为奇数,$(p,b_1)=1$.

由 $p|(2y_0-1)^2+3^2\cdot 11$,得

$p|b_1^2[(2y_0-1)^2+3^2\cdot 11]$,即

$$p|(2b_1y_0-b_1)^2+(3b_1)^2\cdot 11. \tag{②}$$

由①有

$(3b_1)^2\cdot 11=(1-a_1p)^2\cdot 11\equiv 11 \pmod p$.

所以由②有

$p|(2b_1y_0-b_1)^2+11$.

由 b_1 是奇数,可令 $b_1=2m+1$,则

$2b_1y_0-b_1=2(2m+1)y_0-2m-1=2[(2m+1)y_0-m]-1$.

取 $x_0=(2m+1)y_0-m$,就有 $p|(2x_0-1)^2+11$.

于是命题得证.

证法 2 令 $f(x)=x^2-x+3$, $g(y)=y^2-y+25$.

首先,由于对任意整数 x_0 和 y_0,$f(x_0)$和 $g(y_0)$均为奇数,可知素数 2 不具有所述性质,从而 $p\neq 2$.

当 $x_0=3$,$y_0=2$ 时,有

$x_0^2-x_0+3=9$,$y_0^2-y_0+25=27$.

因而 $3|(x_0^2-x_0+3)$,$3|(y_0^2-y_0+25)$.

所以对于 $p=3$ 结论成立.

下设素数 $p\geqslant 5$. 由于

$3^2f(x)=9x^2-9x+27=(3x-1)^2-(3x-1)+25=g(3x-1)$.

因此，若存在整数 x_0，使 $p|f(x_0)$，只要令 $y_0=3x_0-1$，就有 $p|g(3x_0-1)$，亦即 $p|g(y_0)$.

反之，若存在整数 y_0，使 $p|g(y_0)$，则对任意整数 k，有 $p|g(y_0+kp)$.

这是因为

$$g(y_0+kp)=(y_0+kp)^2-(y_0+kp)+25$$
$$=(y_0^2-y_0+25)+2y_0kp-kp+k^2p^2$$
$$\equiv g(y_0)(\bmod p).$$

又由于 $(p,3)=1$，故可取 $k\in\{0,1,2\}$，使

$y_0+kp\equiv 2(\bmod 3)$.

于是只要取 $3x_0-1=y_0+kp$，就有 $x_0=\frac{1}{3}(y_0+kp+1)$ 为整数.

由于 $g(y_0+kp)=g(3x_0-1)=3^2f(x_0)$，及 $p|g(y_0+kp)$，可知

$p|3^2f(x_0)$.

又由于 p 是大于等于 5 的素数，$(p,3^2)=1$，于是

$p|f(x_0)$.

4. 灵活运用威尔逊定理

例 33 设 p 是素数，令 $k=1+2+\cdots+(p-1)$，求证：

$k|(p-1)!-(p-1)$.

证明 由威尔逊定理，有 $p|(p-1)!+1$，知有整数 m，使得 $(p-1)!=mp-1$，即 $(m-1)p=(p-1)!-(p-1)=(p-1)\cdot l$，其中 $l=(p-2)!-1$ 为整数. 于是 $p|(p-1)l$.

而 $(p-1,p)=1$，故 $p|l$，即 $l=np$.

从而，由 $(m-1)p=(p-1)pn$，有 $m-1=n(p-1)$.

故
$$(p-1)!=[n(p-1)+1]p-1=n(p-1)p+p-1$$
$$=2n\cdot\frac{(p-1)p}{2}+p-1=2nk+p-1.$$

即 $k|(p-1)!-(p-1)$.

例 34 (IMO-46 预选题) 设 $P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，其中，$a_0$，$a_1$，$\cdots$，$a_n$ 是整数，$a_n>0(n\geqslant 2)$. 证明：存在正整数 m，使得 $P(m!)$ 是合数.

证明 假设 $a_0=\pm 1$. 否则，当 $a_0=0$ 及 $a_0\neq 0$，± 1 时，结论成立.

若素数 $p>k\geqslant 1$，则

$$(p-1)!=(p-k)![p-(k-1)][p-(k-2)]\cdot\cdots\cdot(p-1)$$
$$\equiv(-1)^{k-1}(p-k)!(k-1)!(\bmod p).$$

由威尔逊(Wilson)定理知

$(p-1)!\equiv-1(\bmod p)$.

所以，$(p-k)!(k-1)!\equiv(-1)^k(\bmod p)$.

设 $Q(x)=a_n+a_{n-1}x+\cdots+a_0x^n$，则有

$$P\left(\frac{(-1)^k}{(k-1)!}\right)=\frac{(-1)^{kn}}{[(k-1)!]^n}Q((-1)^k(k-1)!).$$

若 $k-1>a_n^2$，则 $a_n\mid(k-1)!$，且 $\frac{(k-1)!}{a_n}$ 可以被小于或等于 $k-1$ 的所有的素数整除. 于是，

$Q((-1)^k(k-1)!)=a_nb_k$，

其中，$b_k=1+\frac{a_{n-1}(-1)^k(k-1)!}{a_n}+\cdots+\frac{a_0[(-1)^k(k-1)!]^n}{a_n}$ 中没有小于或等于 $k-1$ 的素因数.

由于 $Q(x)$ 的首项为 $a_0=\pm1$，所以，$Q(x)$ 不是常数.

故当 k 足够大时，$|Q((-1)^k(k-1)!)|$ 也可以足够大.

从而，$|b_k|$ 也可以足够大.

特别地，当 k 足够大时，$|b_k|>1$.

取这样的 k 为偶数，任选 b_k 的素因数 p，则 $p>k$，且有

$P((p-k)!)\equiv0(\bmod p)$.

为了证明原命题，需要确定 k，使得

$|P((p-k)!)|>p$.

取 $k=m!$，其中，$m=q-1>2$，q 是一个素数，则 $m!$ 是合数，$m!+1$ 也是合数[因为 $m!+1>m+1=q$，由威尔逊定理知 $m!+1\equiv0(\bmod q)$]，且 $m!+l(l=2,3,\cdots,m)$ 也是合数.

所以，设比 $m!+l$ 大的最小的素数 $p=m!+m+t(t\geqslant1,t\in\mathbf{N})$.

因此，$p-k=m+t$.

对于足够大的 m，有

$P((p-k)!)=P((m+t)!)>\frac{(m+t)!}{2}$，这是因为 $a_n>0$.

当 m 足够大时，

$\frac{(m+t)!}{2}>m!+m+t(t\geqslant1)$.

因此，$P((p-k)!)>p$，且 $P((p-k)!)$ 是 p 的倍数.

所以，$P((p-k)!)$ 是合数.

5. 借助于素数处理问题

例 35 （1985 年第 3 届美国数学邀请赛题）设 a，b，c，d 是正整数，满足 a^5

b^4，$c^3=d^2$，且 $c-a=19$，求 $d-b$.

解 由 $a^5=b^4$，$c^3=d^2$.

注意到 $(5,4)=1$，$(3,2)=1$，可知，存在两个正整数 m 及 n，使

$a=m^4$，$b=m^5$，$c=n^2$，$d=n^3$.

于是 $19=c-a=n^2-m^4=(n+m^2)(n-m^2)$.

由于 19 是素数，以及 $n-m^2<n+m^2$，则有

$$\begin{cases} n-m^2=1, \\ n+m^2=19. \end{cases}$$

解得 $n=10$，$m=3$.

有 $d=n^3=1000$，$b=m^5=243$.

故 $d-b=1000-243=757$.

例 36 （1978 年基辅数学奥林匹克题）求最小的自然数 a 和 $b(b>1)$，使得 $\sqrt{a\sqrt{a\sqrt{a}}}=b$.

解 由题意得

$$b^8=(\sqrt{a\sqrt{a\sqrt{a}}})^8=a^7. \quad ①$$

设素数 p 能整除 b（因为 $b>1$，所以这样的素数是存在的）.

由①，p 也能整除 a.

设 $b=p^\beta\cdot c$，$a=p^\alpha\cdot d$，这里 c 和 d 都是与 p 互素的自然数，$\alpha\geqslant1$，$\beta\geqslant1$. 从而有

$$p^{8\beta}\cdot c^8=p^{7\alpha}\cdot d^7. \quad ②$$

因为 $(c^8,p)=1$，$(d^7,p)=1$，则由②有

$8\beta=7\alpha$.

又 $(7,8)=1$，则 7 能整除 β，8 能整除 α，因而有

$\alpha\geqslant8$，$\beta\geqslant7$.

又因为 $c\geqslant1$，$d\geqslant1$，$p\geqslant2$，所以必有

$a=p^\alpha\cdot d\geqslant p^\alpha\geqslant p^8\geqslant2^8=256$，

$b=p^\beta\cdot c\geqslant p^\beta\geqslant p^7\geqslant2^7=128$.

因而 $a=256$，$b=128$ 是满足给定等式的最小自然数.

例 37 （1951 年匈牙利数学奥林匹克题）对于怎样的整数 m，乘积 $1\cdot2\cdot3\cdot\cdots\cdot(m-1)$ 能被 m 整除？

解 (1) 如果 $m=p$ 是素数，显然

$p\nmid1\cdot2\cdot3\cdot\cdots\cdot(p-1)$.

(2) 如果 m 可以分解为两个不同的整数的乘积，即可表示成

$m=ab$，$a\neq b$，$a>1$，$b>1$.

显然 $a\leqslant m-1$，$b\leqslant m-1$，于是

$m=ab\mid 1\cdot 2\cdot\cdots\cdot(m-1)$.

(3) 如果 m 只能分解为两个相同因子的乘积，即 m 可表示为素数 p 的平方的形式，设 $m=p^2$.

当 $p\neq 2$ 时，则必有 $p^2>2p$，

于是在 1，2，…，p^2-1 中必有一数为 p，一数为 $2p$. 从而

$2p^2\mid 1\cdot 2\cdot 3\cdot\cdots\cdot(p^2-1)$，即 $p^2\mid 1\cdot 2\cdot 3\cdot\cdots\cdot(p^2-1)$.

也就是 $m\mid 1\cdot 2\cdot 3\cdot\cdots\cdot(m-1)$.

于是，对于除 $m=4$ 之外的任何合数 m，总有

$m\mid 1\cdot 2\cdot 3\cdot\cdots\cdot(m-1)$.

例 38 （1964 年第 4 届全俄数学奥林匹克题）求使 $(n-1)!$ 不能被 n^2 整除的一切奇自然数 n.

解 首先可以证明 n 是奇素数和 $n=9$ 时，$(n-1)!$ 不能被 n^2 整除.

当 n 是奇素数时，则 $(n-1)!$ 中不含有约数 n，因此 $(n-1)!$ 不能被 n^2 整除.

当 $n=9$ 时，显然 8! 能被 9 整除，但不能被 $9^2=81$ 整除.

下面再证明当 n 是奇合数，且 $n\neq 9$ 时，$(n-1)!$ 一定能被 n^2 整除.

如果 n 是奇合数，且不是奇素数的平方.

设 $n=ab$，$a\geqslant 3$，$b\geqslant 3$，$a\neq b$.

这时 a，$2a$，b，$2b$ 必定是乘积 $1\cdot 2\cdot 3\cdot\cdots\cdot(n-1)$ 的因数，所以 $(n-1)!$ 能被 $a^2b^2=n^2$ 整除.

如果 n 是不小于 5 的奇素数的平方.

设 $n=p^2$，p 是素数，$p\geqslant 5$.

这时必有 $p^2-1\geqslant 4p$.

因而在 $(n-1)!=(p^2-1)!$ 中一定有因数 $p,2p,3p,4p$. 因此 $(n-1)!$ 能被 $(p^2)^2=p^4$ 整除.

综上所知，符合题目要求的奇自然数 n 是奇素数和 $n=9$.

例 39 （CMO-21 试题）正整数 a_1，a_2，…，a_{2006}（可以有相同的）使得 $\frac{a_1}{a_2}$，$\frac{a_2}{a_3}$，…，$\frac{a_{2005}}{a_{2006}}$ 两两不相等. 问：a_1，a_2，…，a_{2006} 中最少有多少个不同的数？

解 答案：a_1，a_2，…，a_{2006} 中最少有 46 个互不相同的数.

由于45个互不相同的正整数两两比值至多有 $45\times44+1=1981$ 个，故 a_1，a_2，…，a_{2006} 中互不相同的数大于45.

下面构造一个例子，说明46是可以取到的.

设 p_1，p_2，…，p_{46} 为46个互不相同的素数，构造 a_1，a_2，…，a_{2006} 如下：

p_1，p_1，p_2，p_1，p_3，p_2，p_3，p_1，p_4，p_3，p_4，p_2，p_4，p_1，…，

p_1，p_k，p_{k-1}，p_k，p_{k-2}，p_k，…，p_k，p_2，p_k，p_1，…，

p_1，p_{45}，p_{44}，p_{45}，p_{43}，p_{45}，…，p_{45}，p_2，p_{45}，p_1，

p_{46}，p_{45}，p_{46}，p_{44}，p_{46}，…，p_{46}，p_{22}，p_{46}.

这2006个正整数满足要求.

所以 a_1，a_2，…，a_{2006} 中最少有46个互不相同的数.

【模拟实战】

习题A

1. （1989年第15届全俄数学奥林匹克题）证明数 $4^{545}+545^4$ 是合数.
2. 证明数 $1\underbrace{00\cdots0}_{161个}1$ 是合数.
3. 证明数 $1\underbrace{00\cdots00}_{2^{1974}+2^{1000}-1个0}1$ 是合数.
4. （1987年第13届全俄数学奥林匹克题）证明对于每一个 n，数 $\underbrace{11\cdots1}_{n个}2\underbrace{11\cdots1}_{n个}$ 是合数.
5. （2005年斯洛文尼亚数学奥林匹克题）求最小的素数 p，使得 p^3+2p^2+p 恰有42个因数.
6. （第48届斯洛文尼亚数学奥林匹克题）求所有的素数 p，使得 $p+28$ 与 $p+56$ 也都是素数.
7. （第19届韩国数学奥林匹克题）对 $a\in\mathbf{N}_+$，设 S_a 是满足如下条件的素数的集合：

   对任何 $p\in S_a$，存在奇数 b，使得 $p\mid[(2^{2^a})^b-1]$.

   求证：对所有的 $a\in\mathbf{N}_+$，存在无穷多个素数没有被包含在 S_a 中.
8. （1981年基辅数学奥林匹克题）若数 p，$p+10$，$p+14$ 都是素数，求 p.
9. （1973年基辅数学奥林匹克题）求三个素数，使得它们的积为和的5倍.
10. （1983年第1届美国数学邀请赛题）整数 C_{200}^{100} 的最大的两位数的素因数是多少？

11. （1980年列宁格勒数学奥林匹克题）已知方程 $x^4-px^3+q=0$ 有一整数根，求素数 p 与 q.

习题B

1. （1965年第28届莫斯科数学奥林匹克题）试找出所有的位数不超过19的，具有形状 p^p+1 的素数（p 为自然数）.
2. （1992年乌克兰数学奥林匹克题）试求出所有不超过1000的素数 p，这些 p 使 $2p+1$ 是自然数的方幂（亦即存在自然数 m 和 n，$n\geqslant2$，使得 $2p+1=m^n$）.
3. （1974年基辅数学奥林匹克题）求8个素数（不一定不同），使得它们的平方和比它们的乘积的4倍小992.
4. （1988年第51届莫斯科数学奥林匹克题）设 p_1，p_2，…，p_{24} 是一些不小于5的素数. 证明 $p_1^2+p_2^2+\cdots+p_{24}^2$ 可被24整除.
5. （1968年第31届莫斯科数学奥林匹克题）如果 p 和 q 是两个素数，并且 $q=p+2$. 证明 p^q+q^p 能被 $p+q$ 整除.
6. （1973年第34届美国普特南数学竞赛题）设整数 $p>1$，x 是满足 $0\leqslant x<p$ 的所有整数，使得二次三项式 x^2-x+p 是素数.（例如 $p=5$ 与 $p=41$ 就有这种性质）
   证明存在唯一的整数组 a，b，c 满足 $b^2-4ac=1-4p$，$0<a\leqslant c$，$-a\leqslant b<a$.
7. （1985年中国江苏省苏州市、镇江市高中数学竞赛题）设 p，q 为正素数，方程 $x^2+p^2x+q^3=0$ 有有理根吗？如果没有，给出证明；如果有，请求出来.
8. （1981年保加利亚数学奥林匹克题）证明如果 $1+2^n+4^n$ 是素数，$n\in\mathbf{N}$，则 $n=3^k$，其中 k 是非负整数.
9. （1990年匈牙利数学奥林匹克题）对任一正整数 q_0，考虑由 $q_i=(q_{i-1}-1)^3+3(i=1,2,\cdots,n)$ 定义的序列 $q_1,q_2,\cdots,q_n$. 若每个 $q_i(i=1,2,\cdots,n)$ 都是素数的幂，求 n 的最大的可能值.
10. （2006年波兰数学奥林匹克题）给定素数 p 和正整数 n（$p\geqslant n\geqslant3$）. 集合 A 由元素取自集合 $\{1,2,\cdots,p\}$ 的长度为 n 的序列构成. 若对集合 A 中的任意两个序列 $(x_1,x_2,\cdots,x_n)$ 和 $(y_1,y_2,\cdots,y_n)$，均存在三个不同的正整数 k，l，m，使得 $x_k\neq y_k$，$x_l\neq y_l$，$x_m\neq y_m$. 试求集合 A 中的元素个数的最大值.
11. （2007年东南数学奥林匹克题）试求满足下列条件的素数三元组（a，b，c）：
   （1）$a<b<c<100$，a，b，c 为素数；
   （2）$a+1$，$b+1$，$c+1$ 组成等比数列.

第六章　素因数分解

【基础知识】

1. **素因数分解定理**（整数的唯一分解定理）：每一个大于 1 的整数都能分解成素因数连乘积的形式，并且如果把这些素因数按照由小到大的顺序排列（相同因数的乘积写成幂的形式），这种分解方法是唯一的.

2. 整数 $n(n>1)$ 的标准分解式

$$n=\prod_{i=1}^{m} p_i^{a_i} \qquad ①$$

其中 p_i 为素数，a_i 为正整数，$i=1,2,\cdots,m$.

3. **约数个数定理**：设 $d(n)=\sum\limits_{d\mid n}1$ 表示大于 1 的整数 n 的所有正约数的个数，n 的标准分解式为①式，则

$$d(n)=\prod_{i=1}^{n}(1+a_i).$$

4. **约数和定理**：设 $\sigma(n)=\sum\limits_{d\mid n}d$ 表示大于 1 的整数 n 的所有正约数的和，n 的标准分解式为①式，则

$$\sigma(n)=\prod_{i=1}^{m}\frac{p_i^{a_i+1}-1}{p_i-1}.$$

5. 在 $n!$ 的标准分解式中，素因数 p 的方幂为 $\sum\limits_{r=1}^{\infty}\left[\frac{n}{p^r}\right]$.

其中记号$[x]$表示不超过 x 的最大整数.

【典型例题与基本方法】

例 1　（1988 年奥地利数学竞赛题）求 $N=19^{88}-1$ 的所有形如 $d=2^a\cdot 3^b$（a，b 为自然数）的因子 d 之和.

解　$N=19^{88}-1=(20-1)^{88}-1=(4\cdot 5-1)^{88}-1$

$$=-C_{88}^1 4\cdot 5+C_{88}^2 4^2\cdot 5^2-C_{88}^3 4^3\cdot 5^3+\cdots-C_{88}^{87}4^{87}5^{87}+C_{88}^{88}4^{88}5^{88}$$

$$=-2^5\cdot 55+2^6M=2^5(-55+2M),$$

其中 M 为整数.

所以，N 的标准分解式中，2 的最高次幂是 5.

另一方面，

$$
\begin{aligned}
N &= (2\cdot 9+1)^{88}-1 \\
&= C_{88}^{1}2\cdot 9+C_{88}^{2}2^{2}\cdot 9^{2}+\cdots+C_{88}^{88}2^{88}\cdot 9^{88} \\
&= 3^{2}\cdot 2\cdot 88+3^{3}\cdot T \\
&= 3^{2}(2\cdot 88+3T),
\end{aligned}
$$

其中 T 为整数.

所以，在 N 的标准分解式中，3 的最高次幂是 2，即

$N=2^{5}\cdot 3^{2}\cdot L$,

其中 L 中没有因数 2 和 3.

于是，N 中所有形如 $d=2^{a}\cdot 3^{b}$ 的因子之和为

$(2+2^{2}+2^{3}+2^{4}+2^{5})(3+3^{2})=744$.

例 2 （2003 年泰国数学奥林匹克题）求所有使 $p^{2}+2543$ 具有少于 16 个不同正因子的素数 p.

解 设 $p(p>3)$是一个素数. 易证 $p^{2}-1$ 能被 24 整除.

易看出 $p^{2}+2543=p^{2}-1+106\times 24$ 是 24 的倍数.

令 $p^{2}+2543=24k$ （$k\in\mathbf{N}$，$k\geqslant 107$）.

设 $k=2^{r}\times 3^{s}\times k'$，其中 r，s 为非负整数，k'是使得$(k',6)=1$ 的正整数，又设 $T(n)$是 n 的所有正因子的个数，显见

$T(p^{2}+2543)=T(2^{3+r}\times 3^{1+s}\times k')=(4+r)(2+s)T(k')$.

当 $k'>1$ 时，$T(k')\geqslant 2$，即

$T(p^{2}+2543)\geqslant 16$.

当 $k'=1$ 时，

$T(p^{2}+2543)=(4+r)(2+s)$.

如果 $T(p^{2}+2543)<16$，则 $r\leqslant 3, s\leqslant 1$，故 $k=2^{r}\times 3^{s}\leqslant 24$，与 $k\geqslant 107$ 矛盾.

所以，对所有的素数 $p(p>3)$，有

$T(p^{2}+2543)\geqslant 16$.

考虑

$T(2^{2}+2543)=T(2547)=T(3^{2}\times 283)=6$,

$T(3^{2}+2543)=T(2552)=T(2^{3}\times 11\times 29)=16$,

只有 $p=2$ 满足 $T(p^{2}+2543)<16$.

因此，所求的素数为 2.

例 3 （第 36 届加拿大数学奥林匹克题）设 T 为 2004^{100} 的所有正约数的集合，T 的子集 S 满足 S 中的元素不是 S 中其他任意元素的整数倍．求 S 的元素个数的最大可能值．

解 因为 $2004=2^2\times3\times167$，所以，

$T=\{2^a\times3^b\times167^c\mid0\leqslant a\leqslant200,0\leqslant b,c\leqslant100,\forall a,b,c\in\mathbf{N}\}$．

设 $S=\{2^p\times3^q\times167^r\}$，这里 p 是某些不超过 200 的自然数，q，r 是某些不超过 100 的自然数．

构造满足题设的 T 的子集 S：

当 q，r 确定时，p 的取值是唯一确定的．令 $p=200-q-r$，当 q，r 分别取遍所有不超过 100 的自然数，即 $0\leqslant q$，$r\leqslant100$ 时，p 都满足 $0\leqslant p\leqslant200$．

从而，取 $S=\{2^{200-b-c}\times3^b\times167^c\mid0\leqslant b,c\leqslant100,\forall b,c\in\mathbf{N}\}$．

由于 b，c 均有 101 个可能值，故 $|S|=101^2$．

下面证明，S 中任意一个元素都不是其他元素的倍数，并且 T 没有更多元素的子集满足题设．

(1) 设 S 中的某两个元素 $2^{200-b-c}\times3^b\times167^c$，$2^{200-s-t}\times3^s\times167^t$，其中 $2^{200-b-c}\times3^b\times167^c$ 是 $2^{200-s-t}\times3^s\times167^t$ 的整数倍，则

$200-b-c\geqslant200-s-t$，$b\geqslant s$，$c\geqslant t$．

从而，由第一个不等式，得 $b+c\leqslant s+t$；

而由第二、三个不等式，得 $b+c\geqslant s+t$．

故 $b+c=s+t$．

因此，以上各不等式取等号，即 $b=s$，$c=t$．矛盾．

于是，S 中任一元素不是其他元素的倍数．

(2) 设 U 是 T 的一个子集，且其元素个数多于 101^2．

因为 $0\leqslant b$，$c\leqslant100$，所以，仅有 101^2 个不同的整数对 (b,c)．从而，由抽屉原理，U 中至少有两个元素 $u_1=2^{a_1}\times3^{b_1}\times167^{c_1}$ 与 $u_2=2^{a_2}\times3^{b_2}\times167^{c_2}$，且 $b_1=b_2$，$c_1=c_2$，但 $a_1\neq a_2$．

若 $a_1>a_2$，则 u_1 是 u_2 的倍数；

若 $a_1<a_2$，则 u_2 是 u_1 的倍数．

于是，U 不满足题设．

因此，所求最大值为 $101^2=10\ 201$．

例 4 （第 34 届美国数学奥林匹克题）求所有的正整数 n，满足 n 为合数，且其所有大于 1 的因数可以放在一个圆上，使得任意两个相邻的因数都不是互素的．

解 若 $n=pq$，其中 p，q 为不同的素数，则其大于 1 的因数为 p，q，pq，无论

怎样放在圆周上，p 和 q 总会相邻，且 p 和 q 互素，不满足要求.

若 $n=p^m$，其中 p 为素数，正整数 $m\geqslant 2$，则无论怎样将 n 的大于 1 的因数放在一个圆上，任意两个相邻的因数都不互素.

若 $n=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$，其中素数 $p_1<p_2<\cdots<p_k$，m_1，m_2，…，m_k 为正整数，且 $k>2$ 或 $k=2$ 时，$\max\{m_1,m_2\}>1$.

设 $D_n=\{d\,|\,d|n,且\ d>1\}$.

首先，将 n，p_1p_2，p_2p_3，…，$p_{k-1}p_k$ 按顺时针放在圆上. 在 n 和 p_1p_2 之间依任意的次序放入 D_n 中所有以 p_1 为最小素因数的正整数（不包括 p_1p_2）；在 p_1p_2 和 p_2p_3 之间，依任意的次序放入 D_n 中所有以 p_2 为最小素因数的正整数（不包括 p_2p_3）；继续以这种方法放置，最后，在 $p_{k-1}p_k$ 和 n 之间，依任意的次序放入 p_k，p_k^2，…，$p_k^{m_k}$. 于是，D_n 中的所有元素恰被放在圆周上一次，且任意相邻的两个数有一个公共的素因数.

因此，这样安排满足要求.

例 5 （IMO-31 预选题）整数 9 可以表示成两个连续整数之和：$9=4+5$. 同时，9 可以用两种不同的方法写成连续自然数的和：$9=4+5=2+3+4$.

问是否有这样的自然数 N：

(1) 它是 1990 个连续整数的和；

(2) 它恰能以 1990 种不同的方法表示成连续整数的和.

解 如果条件 (1) 被满足，则

$$\begin{aligned}N&=n+(n+1)+(n+2)+\cdots+(n+1989)\\&=\frac{1}{2}\cdot 1990(2n+1989)\\&=995(2n+1989).\end{aligned} \quad ①$$

由①，N 必为奇数.

设 N 可以写成 $k+1$ 个(k 为自然数)连续自然数之和，且这 $k+1$ 个数中最小者为 m，则

$$\begin{aligned}N&=m+(m+1)+\cdots+(m+k)\\&=\frac{1}{2}(k+1)(2m+k),\end{aligned}$$

即 $$2N=(k+1)(2m+k). \quad ②$$

由①有

$$1990(2n+1989)=(k+1)(2m+k).$$

因此，满足上式的(m,k)有多少对，则 N 就有多少种方法写成连续 $k+1$ 个自然数之和.

由②及 m 是自然数可知

$k+1|2N$， $k+1<k+2m$.

所以 $k+1<\sqrt{2N}$.

反之，如果有一个 $2N$ 的约数 $<\sqrt{2N}$，记这个约数为 $k+1$，则

$2N=(k+1)c$.

其中 $k+1<c$.

可以把 c 记为 $2m+k$，$m\in\mathbf{N}$.

因为 N 是奇数，所以 $k+1$ 与 c 不可能都是偶数. 因此，当 k 是奇数时，c 是奇数；当 k 是偶数时，c 是偶数. 因此可以把 c 记为 $2m+k$.

于是 $2N=(k+1)(2m+k)$.

这就说明，当 N 为奇数时，若 N 可以写成多于一个的连续自然数之和的形式有 l 种，则 l 就是 $2N$ 的大于 1 且小于 $\sqrt{2N}$ 的约数的个数.

由① $N=995(2n+1989)$，得

$2N=1990(2n+1989)=2\cdot 5\cdot 199(2n+1989)=2^1\cdot 5^a\cdot 199^b p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k}$.

由于 N 有 1990 种不同的分法，把 1 个自然数的情况考虑在内，则 $2N$ 的约数个数为

$(1+1)(a+1)(b+1)(b_1+1)\cdot\cdots\cdot(b_k+1)=2\cdot 1991=2\cdot 11\cdot 181$.

其中 $a,b\in\mathbf{N}$，$b_i\in\mathbf{N}\cup\{0\}$，$i=1,2,\cdots,k$.

于是 $b_1=b_2=\cdots=b_k=0$，从而

$(a+1)(b+1)=11\cdot 181$，则

$\begin{cases}a=10,\\b=180,\end{cases}$ 或 $\begin{cases}a=180,\\b=10.\end{cases}$

即 $N=5^{10}\cdot 199^{180}$ 或 $N=5^{180}\cdot 199^{10}$.

例 6 （CMO－5 试题）设 x 是一个自然数，若一串自然数 $x_0=1$，x_1，x_2，…，$x_l=x$，满足 $x_{i-1}<x_i$，$x_{i-1}|x_i$，$i=1,2,\cdots,l$，则称 $\{x_0,x_1,x_2,\cdots,x_l\}$ 为 x 的一条因子链，l 为该因子链的长度，$L(x)$ 与 $R(x)$ 分别表示 x 的最长因子链的长度和最长因子链的条数.

对于 $x=5^k\cdot 31^m\cdot 1990^n$（$k,m,n$ 是自然数），试求 $L(x)$ 与 $R(x)$.

解 对于任意自然数

$x=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，

其中 p_1，p_2，…，p_n 为互不相同的素数，α_1，α_2，…，α_n 为正整数.

显然，x 的因子链存在且只有有限点，从而一定存在最长因子链.

设$\{x_0,x_1,\cdots,x_t\}$为x的一个最长因子链，我们证明$\frac{x_i}{x_{i-1}}$必为素数$(i=1,2,\cdots,t)$.

事实上，如果存在i $(1\leqslant i\leqslant t)$ 使得$\frac{x_i}{x_{i-1}}$不是素数，可设

$$\frac{x_i}{x_{i-1}}=q_1q_2,$$

其中q_1，q_2都是大于1的正整数，则

$$\{x_0,x_1,\cdots,x_{i-1},q_1x_{i-1},x_i,x_{i+1},\cdots,x_t\}$$

也是x的一个因子链.

这与$\{x_0,x_1,\cdots,x_{i-1},x_i,\cdots,x_t\}$是最长因子链相矛盾.

由此可知，对任何$1\leqslant i\leqslant t$，$\frac{x_i}{x_{i-1}}$必是x的一个素因子，从而

$$t=L(x)=\alpha_1+\alpha_2+\cdots+\alpha_n.$$

反之，如果$\{x_0,x_1,\cdots,x_m\}$为x的一个因子链，而且对任何$1\leqslant i\leqslant m$，$\frac{x_i}{x_{i-1}}$都是素数，由因子链的定义可知

$$m=\alpha_1+\alpha_2+\cdots+\alpha_n=L(x).$$

即$\{x_0,x_1,\cdots,x_m\}$必为最长因子链.

因此，从1开始逐次乘x的一个素因子直到达到x为止，就得到x的一个最长因子链，而且不同素因子乘的顺序不同得到不同的最长因子链，因而

$$R(x)=\frac{(\alpha_1+\cdots+\alpha_n)!}{\alpha_1!\cdot\cdots\cdot\alpha_n!}$$

对于$x=5^k\cdot31^m\cdot1990^n=2^n\cdot5^{k+n}\cdot31^m\cdot199^n$.

则$L(x)=3n+k+m$,

$$R(x)=\frac{(3n+k+m)!}{(n!)^2m!\ (k+n)!}.$$

【解题思维策略分析】

1. 求解满足某些正因数条件的正整数

例7 （1982年基辅数学奥林匹克题）求自然数N，使得它能被5和49整除，并且包括1和N在内，它共有10个约数.

解 把数N写成素因数分解的形式：

$$N=2^{\alpha_1}\cdot3^{\alpha_2}\cdot5^{\alpha_3}\cdot7^{\alpha_4}\cdot\cdots\cdot p_n^{\alpha_n},$$

其中$\alpha_i\geqslant0$，$i=1,2,\cdots,n$.

则它的所有约数的个数为

$(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)(\alpha_4+1)\cdot\cdots\cdot(\alpha_n+1)=10.$

由于 $5|N, 7^2|N$，则

$\alpha_3+1\geqslant 2,\ \alpha_4+1\geqslant 3.$

因此 $\alpha_1, \alpha_2, \alpha_5, \cdots, \alpha_n$ 必然都等于 0，即

$N=5^{\alpha_3}\cdot 7^{\alpha_4}.$

由 $(\alpha_3+1)(\alpha_4+1)=10=2\cdot 5$，可得

$\alpha_3=1,\ \alpha_4=4.$

即本题有唯一解 $N=5\cdot 7^4$.

例 8 （IMO－26 预选题）求最小的正整数 n，满足：

(1) n 恰有 144 个不同的正因数；

(2) 在 n 的正因数中有 10 个连续整数.

解 由于 10 个连续整数中必有数被 2^3，3^2，5，7 整除，所以其中 $\alpha_1\geqslant 3$，$\alpha_2\geqslant 2$，$\alpha_3\geqslant 1$，$\alpha_4\geqslant 1$，….

由于 n 的正因数个数为

$(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)(\alpha_4+1)(\alpha_5+1)\cdots=144$，

而 $(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)(\alpha_4+1)\geqslant 4\cdot 3\cdot 2\cdot 2=48$，

于是有 $(\alpha_5+1)\cdots\leqslant 3$.

所以至多有一个 $\alpha_j(j\geqslant 5)$ 为正数，并且 α_j 只能等于 1 或 2.

考虑方程 $(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)(\alpha_4+1)(\alpha_5+1)=144$ 关于 $\alpha_1\geqslant 3, \alpha_2\geqslant 2, \alpha_3\geqslant 1, \alpha_4\geqslant 1, \alpha_5=1$ 或 2 的所有的解，并使 n 最小，由此可得

$\alpha_1=5,\ \alpha_2=2,\ \alpha_3=\alpha_4=\alpha_5=1.$

即 $n=2^5\cdot 3^2\cdot 5\cdot 7\cdot 11=110880$.

此时 n 有连续正因数 1，2，3，…，11，12.

例 9 （1999 年加拿大数学奥林匹克题）确定所有的正整数 n，满足 $n=[d(n)]^2$，其中 $d(n)$ 表示 n 的所有正约数的个数（包括 1 及其本身）.

解 设 n 的标准分解式为 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$（$p_i$ 是素数，$\alpha_i\geqslant 0$），有

$d(n)=(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_k).$

由题意，$n=[d(n)]^2$，则 n 为完全平方数，α_i 为偶数，记 $\alpha_i=2\beta_i$，于是

$p_1^{2\beta_1}p_2^{2\beta_2}\cdots p_k^{2\beta_k}=(1+2\beta_1)^2(1+2\beta_2)^2\cdots(1+2\beta_k)^2$，即

$$p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}=(1+2\beta_1)(1+2\beta_2)\cdots(1+2\beta_k). \quad (*)$$

上式右边是奇数，于是 p_i 为奇素数，$p_i\geqslant 3$.

当 $\beta_i>0$ 时，有 $p_i^{\beta_i}\geqslant 3^{\beta_i}=(1+2)^{\beta_i}>1+2\beta_i$，

$$p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}>(1+2\beta_1)(1+2\beta_2)\cdots(1+2\beta_k). \quad (**)$$

(*)式与(**)式矛盾.

故对所有 i，$\beta_i=0$. 因此 $n=1$.

例 10 （1988 年加拿大数学奥林匹克训练题）已给一个正整数的所有正因数的乘积，是否总能唯一确定这个正整数?

解 设 d 为 n 的因数，则 $\frac{n}{d}$ 也是 n 的因数.

又设 $P(n)$为 n 的所有正因数的乘积，即

$$P(n)=\prod_{d\mid n}d.$$

又有 $P^2(n)=\prod_{d\mid n}d\cdot\prod_{d\mid n}\frac{n}{d}=n^{\tau(n)}$，

其中 $\tau(n)$是 n 的正因数的个数. 从而

$$P(n)=n^{\frac{\tau(n)}{2}}.$$

若有 m，n 满足 $m^{\frac{\tau(m)}{2}}=n^{\frac{\tau(n)}{2}}$，即

$$m^{\tau(m)}=n^{\tau(n)}. \qquad ①$$

这表明，m 和 n 的素因数完全相同，并且每个素因数 p 在 m 的分解式中出现的次数与 n 的分解式中出现的次数的比是 $\tau(n):\tau(m)$.

若 $\tau(n)>\tau(m)$，则每一个素因数 p 在 m 的分解式中出现的次数大于在 n 的分解式中出现的次数，从而 m 的因数个数 $\tau(m)$大于 n 的因数个数 $\tau(n)$，出现矛盾，所以 $\tau(n)\leqslant\tau(m)$.

同理，$\tau(n)\geqslant\tau(m)$.

于是，$\tau(n)=\tau(m)$.

从而由①式得　$m=n$.

因此由因数的乘积 $P(n)=n^{\frac{\tau(n)}{2}}$ 可以唯一确定 n.

例 11 （1989 年第 23 届全苏数学奥林匹克题）自然数 N 恰有 12 个正约数（包括 1 和 N），将它们按递增顺序编号：$d_1<d_2<\cdots<d_{12}$. 已知下标为 d_4-1 的正约数等于$(d_1+d_2+d_4)\cdot d_8$. 试求自然数 N.

解 由 N 的所有正约数满足 $d_1<d_2<\cdots<d_{12}$，可知

$$d_1d_{12}=d_2d_{11}=d_3d_{10}=d_4d_9=d_5d_8=d_6d_7,$$

且 N 至多有 3 个素约数.

记 $d_4-1=k$.

由题设可知 $d_1+d_2+d_4$ 是 d_k 的约数，所以 $d_1+d_2+d_4$ 也是 N 的约数，并且 $d_1+d_2+d_4\geqslant d_5$.

于是就有 $d_k=(d_1+d_2+d_4)\cdot d_8\geqslant d_5d_8=N$.

另一方面，$d_k \leqslant N$.

于是 $d_k = N$.

从而有 $k=12$，$d_4=13$，$d_5=d_1+d_2+d_4$.

又 $d_1=1$，则 $d_5=d_1+d_2+d_4=d_2+14$.

由于 d_2 是素数，并且 $d_2 \leqslant d_4-2=11$.

于是可对 $d_2=2, 3, 5, 7, 11$ 讨论.

若 $d_2=2$，则 $d_5=16=2^4$，N 的约数中还应有 2^2，2^3 等，这是不可能的.

若 $d_2=5$，则 $d_5=19$，此时 N 的约数中已有 3 个素数 5，13，19，则 d_3 应为合数，且其约数为 5，13 或 19，然而对于 $5<d_3<13$ 是不可能的.

若 $d_2=7$，则 $d_5=21$，此时 d_3 需满足 $7<d_3<13$ 且有约数 3，7 或 13，这是不可能的.

若 $d_2=11$，则 $d_5=25$，此时 d_3 满足 $11<d_3<13$，则 $d_3=12$，这时 N 的约数中还应有 2，3，4，5，且应在 d_1 与 d_2 之间，这是不可能的.

所以 $d_2=3$，此时 $d_5=17$，又因为 N 的约数中至多有三个素数，且 $3<d_3<13$，因此只有 $d_3=3^2=9$. 这时

$$N=3^2 \cdot 13 \cdot 17=1989.$$

它恰有 12 个正约数.

2. 利用素因数分解求解各类问题

例 12 （1991 年日本数学奥林匹克题）试求不定方程 $\frac{1}{x+1}+\frac{1}{y}+\frac{1}{(x+1)y}=\frac{1}{1991}$ 的正整数解.

解 已知方程可化为

$$1991y+1991(x+1)+1991=(x+1)y,$$

$$(x+1)y-1991(x+1)-1991y=1991,$$

$$(x+1)y-1991(x+1)-1991y+1991^2=1991+1991^2,$$

$$[(x+1)-1991](y-1991)=1991 \cdot 1992.$$

显然，已知方程的正整数解的个数等价于 $1991 \cdot 1992$ 的正约数的个数，由于

$$1991 \cdot 1992=2^3 \cdot 3 \cdot 11 \cdot 83 \cdot 181,$$

所以 $1991 \cdot 1992$ 有

$$(3+1)(1+1)(1+1)(1+1)(1+1)=64$$

个正约数，即已知方程有 64 组正整数解.

例 13 （2004—2005 年度匈牙利数学奥林匹克题）求最大的整数 k，使得 k 满足下列条件：对于所有的整数 x，y，如果 $xy+1$ 能被 k 整除，则 $x+y$ 也能被 k

整除.

解 只须考虑 $k=\prod_i p_i^{\alpha_i}$（p_i 是素数，$\alpha_i\geqslant 0$）.

取 $(x,k)=1$，则存在 $m\in\mathbf{Z}_+$，且 $1\leqslant m\leqslant k-1$，使得 $mx^2\equiv-1\pmod k$.

令 $y=mx$，则 $k\mid(xy+1)$.

由条件有 $k\mid(x+y)$，即 $k\mid(m+1)x$.

所以，$k\mid(m+1)x^2$.

又 $k\mid(mx^2+1)$，则 $k\mid(x^2-1)$.

故 $x^2\equiv1\pmod{p_i}$，对任意 p_i、$x(p_i\nmid x)$ 均成立.

因此，$p_i=2$ 或 3，$k=2^\alpha\times3^\beta$.

又对任意 x，$2\nmid x$，有 $x^2\equiv1\pmod{2^\alpha}$.

故 $\alpha\leqslant3$（注意到任意奇数的平方模 8 余 1，而模 16 则没有这样的性质）.

同理，$\beta\leqslant1$.

所以，$k\leqslant8\times3=24$.

下面证明：24 满足要求.

若存在 x、$y\in\mathbf{Z}_+$，使 $24\mid(xy+1)$，则

$(x,24)=1$，$(y,24)=1$.

x、$y\equiv1,5,7,11,13,17,19,23\pmod{24}$.

由于对固定的 a，$ax\equiv-1\pmod{24}$在模 24 下有且仅有一解，且 $xy\equiv-1\pmod{24}$，于是，

$x\equiv1\pmod{24}$，$y\equiv23\pmod{24}$；

$x\equiv5\pmod{24}$，$y\equiv19\pmod{24}$；

$x\equiv7\pmod{24}$，$y\equiv17\pmod{24}$；

$x\equiv11\pmod{24}$，$y\equiv13\pmod{24}$.

无论取哪种情况，均有 $24\mid(x+y)$.

故 $k=24$ 即为所求.

例 14 （1984 年第 13 届美国数学奥林匹克题）任何一组 m 个非负数的积的 m 次方根是这 m 个非负数的几何平均数.

(1) 对于哪些正整数 n，有 n 个不同正整数的有限集合 S_n，使得 S_n 的任何子集的几何平均数都是整数?

(2) 有没有不同正整数的无限集合 S，能使 S 的任何有限子集的几何平均数都是整数?

解 (1) m 个非负数的积的 m 次方根是整数的一个充分条件是：

已知的 m 个数都是非负整数的幂，并且幂指数是 m 的正整数倍数.

由于 n 个不同正整数的集合 S_n 的任意非空子集可以含有 1 个，或 2 个，…，或 n 个元素，只要这些元素是正整数的幂，并且幂指数是 1，2，3，…，n 的正整数倍，例如幂指数是 $n!$，这时任何非空子集的几何平均数就是整数.

因此，对于每一个正整数 n，都有 n 个不同正整数为元素的有限集合 S_n 满足要求，因为总有 n 个不同的正整数的 $n!$ 次幂可以作为 S_n 的元素.

(2) 这样的无限集合 S 不存在.

我们用反证法.

设有不同正整数的无限集合 S，它的任何有限子集的几何平均数都是整数.

我们从这些数所含素因数的幂指数来寻找矛盾.

若数 a 的标准分解式为

$$a=\prod_{i=1}^{t} p_i^{k_i}$$

其中 p_i 为素数，k_i 为正整数，$i=1, 2, \cdots, t$.

并对素数 p_i 的指数 k_i 记作

$e(p_i, a)=k_i$.

显然，$p^k \| a$，即 $p^k | a$，且 $p^{k+1} \nmid a$.

设 a，b 是 S 中的两个不同的元素.

因为 $a \neq b$，所以至少有一个素数 p，使得

$e(p, a) \neq e(p, b)$.

依假设，对任意正整数 m，S 有 m 元子集 $\{a, n_1, n_2, \cdots, n_{m-1}\}$ 和 $\{b, n_1, n_2, \cdots, n_{m-1}\}$，此时素数 p 在子集里各数中的指数之和应该是 m 的倍数，即

$e(p, a)+e(p, n_1)+\cdots+e(p, n_{m-1})$ 和 $e(p, b)+e(p, n_1)+\cdots+e(p, n_{m-1})$

都应该是 m 的倍数，从而它们的差即 $e(p, a)-e(p, b)$ 也是 m 的倍数.

由于 m 是任意的，所以只有 0 才是任意正整数的倍数，从而

$e(p, a)-e(p, b)=0$，即 $e(p, a)=e(p, b)$.

这与 $e(p, a) \neq e(p, b)$ 相矛盾.

所以这样的无限集合 S 不存在.

例 15 （2004 年澳大利亚数学奥林匹克题）(1) 已知素数集 $M=\{p_1, p_2, \cdots, p_k\}$. 证明：分母是 M 的所有元素的幂的积（即分母能被 M 的所有元素整除，但不能被其他任何素数整除）的单位分数（即形如 $\frac{1}{n}$ 的分数）的和也是单位分数.

(2) 如果 $\frac{1}{2004}$ 是和中的单位分数，求这个和.

(3) 如果 $M=\{p_1, p_2, \cdots, p_k\}$，$k>2$，证明：和小于 $\frac{1}{N}$，其中 $N=2\times 3^{k-2}(k-2)!$.

解 (1) 考虑的和中作为一个分式的分母出现的每个正整数 n 为 $n=\prod_{j=1}^{k}p_j^{e_j}$，此处，对所有 j，$e_j\geqslant 1$.

由给定素数集合 M 确定的所有单位分数的和为

$$\sum\frac{1}{n}=\sum\frac{1}{\prod_{j=1}^{k}p_j^{e_j}}=\prod_{j=1}^{k}\sum_{e=1}^{\infty}\frac{1}{p_j^e}=\prod_{j=1}^{k}\frac{\frac{1}{p_j}}{1-\frac{1}{p_j}}=\frac{1}{\prod_{j=1}^{k}(p_j-1)}.$$

正如所求的，这也是一个单位分数.

(2) 因为 2004 的素数分解式为

$2004=2^2\times3\times167$,

因此，相应的素数集为 $M=\{2,3,167\}$.

由此得分式的和为

$$\frac{1}{(2-1)(3-1)(167-1)}=\frac{1}{1\times2\times166}=\frac{1}{332}.$$

(3) 注意到 $p\equiv\pm1\pmod 6$ 适用于大于 3 的所有素数 p，否则 p 能被 2 或 3 整除.

在任意连续 6 个大于 3 的整数中，至多有 2 个素数. 考虑素数序列

$\{\overline{p_i}\}=\{2,3,5,7,11,13,\cdots\}$.

用数 $3j+1$ 替换大于 3 的素数 $\overline{p_{j+2}}$，$j=1,2,\cdots$，得数列

$\{\overline{q_i}\}=\{2,3,4,7,10,13,\cdots,3(i-2)+1,\cdots\}$.

对于所有 i，有 $\overline{q_i}\leqslant\overline{p_i}$.

对于 $k>2$ 的给定素数集合 $M=\{p_1,p_2,\cdots,p_k\}$，可得

$$\frac{1}{\prod_{j=1}^{k}(p_j-1)}\leqslant\frac{1}{\prod_{j=1}^{k}(\overline{p_j}-1)}<\frac{1}{\prod_{j=1}^{k}(\overline{q_j}-1)}$$

$$=\frac{1}{1\times2\times3\times6\times\cdots\times3(k-2)}=\frac{1}{2\times3^{k-2}\times(k-2)!}.$$

正如所要求的.

例 16 (第 28 届巴西数学奥林匹克题) 若正整数有 8 个正因数，且这 8 个正因数的和为 3240，则称这个正整数是“好数”. 例如，2006 是好数，因为其因数 1，2，17，34，59，118，1003，2006 的和为 3240. 求好数的最小值.

解 设 $n=\prod_{i=1}^{k}p_i^{\alpha_i}$，其中，$p_1<p_2<\cdots<p_k$ 为素数且对任意的 i，$\alpha_i\geqslant1$. 故

$\prod_{i=1}^{k}(1+\alpha_i)=8.$

当 $k=1$ 时，$\alpha_1=7$；

当 $k=2$ 时，$\alpha_1=1$，$\alpha_2=3$ 或 $\alpha_1=3$，$\alpha_2=1$；

当 $k=3$ 时，$\alpha_1=\alpha_2=\alpha_3=1$；

当 $k\geqslant 4$ 时，无解.

(1) 若 $n=p^7$，p 为素数，则

$$\sum_{i=0}^{7}p^i=3240.$$

(i) 若 $p\geqslant 3$，则

$$\sum_{j=0}^{7}p^j\geqslant\sum_{j=0}^{7}3^j=\frac{3^8-1}{2}=3280>3240.$$

(ii) 若 $p=2$，则 $\prod_{j=0}^{7}p^j=2^8-1=511\neq 3240.$

(2) 若 $n=p^3q$，p、q 为素数，且 $p\neq q$，则有

$(1+p+p^2+p^3)(1+q)=3240$，

$(1+p)(1+p^2)(1+q)=3240=2^3\times 3^4\times 5.$

由 $q\geqslant 2$，得 $1+q\geqslant 3$，从而，

$1+p+p^2+p^3\leqslant 1080.$

进而，$p^3\leqslant 1080\Rightarrow p\leqslant 10\Rightarrow p=2,3,5,7.$

(i) 若 $p=5$，则 $1+p^2=26\nmid 3240$，矛盾.

(ii) 若 $p=7$，则 $1+p^2=50\nmid 3240$，矛盾.

(iii) 若 $p=2$，则 $1+q=\frac{3240}{3\times 5}=216$，从而，$q=215$，矛盾.

(iv) 若 $p=3$，则 $1+q=\frac{3240}{4\times 10}=81$，从而，$q=80$，矛盾.

(3) 若 $n=pqr$，则有

$(1+p)(1+q)(1+r)=3240=2^3\times 3^4\times 5.$

不妨设 $p<q<r$.

(i) 若 $p=2$，则

$(1+q)(1+r)=2^3\times 3^3\times 5.$

注意到要让 pqr 尽量小，则 qr 应尽量小，于是，

$qr=(1+q)(1+r)-(q+1)-(r+1)+1.$

因此，$(q+1)+(r+1)$ 尽量大.

所以，q 尽量小，r 尽量大.

又当 $q=3$ 时，$r=269$. 此时，

$n_{\min}=2\times3\times269=1614$.

(ii) 若 $p\geqslant3$，则

$$\frac{1+p}{2}\cdot\frac{1+q}{2}\cdot\frac{1+r}{2}=3^4\times5.$$

又 $\frac{1+p}{2},\frac{1+q}{2},\frac{1+r}{2}\in(\mathbf{Z}_+\backslash\{1\})$，可能的情况只有：

$\frac{1+p}{2}=3$，$\frac{1+q}{2}=5$，$\frac{1+r}{2}=3^3$ 或 $\frac{1+p}{2}=3$，$\frac{1+q}{2}=3^2$，$\frac{1+r}{2}=3\times5$.

对应的 $(p,q,r)=(5,9,53)$ 或 $(5,17,29)$.

又 9 不是素数，因此，

$(p,q,r)=(5,17,29)$，$n=5\times17\times29=2465$.

综上所述，知 $n_{\min}=1614$.

【模拟实战】

1. 证明正整数 n 的正约数的个数不超过 $2\sqrt{n}$.
2. （1989 年澳大利亚数学竞赛题）设正整数 n 的不同因数的个数为 $N(n)$，例如 24 有因数 1,2,3,4,6,8,12,24，所以 $N_{(24)}=8$. 试确定和

   $$N_{(1)}+N_{(2)}+\cdots+N_{(1989)}$$

   是奇数还是偶数.
3. 假设 $n=2^{p-1}(2^p-1)$，这里 2^p-1 是素数. 证明数 n 的所有不等于 n 本身的约数之和恰好等于 n.
4. （1990 年第 8 届美国数学邀请赛题）n 是满足下列条件的正整数中最小的数：

   (1) n 是 75 的倍数.

   (2) n 恰有 75 个正整数因子（包括 1 及本身).

   试求 $\frac{n}{75}$.
5. （第 30 届美国普特南数学竞赛题）设 n 为自然数，$n+1$ 能被 24 整除，求证 n 的全体约数之和也能被 24 整除.
6. （IMO－45 预选题）设 $\tau(n)$ 表示正整数 n 的正因数的个数. 证明：存在无穷多个正整数 a，使得方程 $\tau(an)=n$ 没有正整数解 n.
7. （2005 年土耳其国家队选拔赛题）证明：对于所有的整数 a_1，a_2，…，a_n，$n>2$，$\prod\limits_{1\leqslant i<j\leqslant n}(a_j-a_i)$ 能被 $\prod\limits_{1\leqslant i<j\leqslant n}(j-i)$ 整除.

8. (2004 年澳大利亚数学奥林匹克竞题) 非负整数数列$\{x_n\}$定义为：x_1 是小于 204 的非负整数，且 $x_{n+1}=\left(\frac{n}{2004}+\frac{1}{n}\right)x_n^2-\frac{n^3}{2004}+1$，$n>0$.

   证明：数列$\{x_n\}$一定包含无数个素数.

9. (2007 年保加利亚国家数学竞赛题) 对于每个正整数 n，定义 a_n 为一位数，且对于 $n>2007$，n 的正因数的数目若为偶数，则 $a_n=0$；n 的正因数的数目若为奇数，则 $a_n=1$. 问：数 $\alpha=0.a_1a_2\cdots a_k\cdots$是有理数吗？

第七章　整数的可除性特征

【基础知识】

1. 一个整数能被 2 整除的充分必要条件是这个数的个位数是偶数.

2. 一个整数能被 4 整除的充分必要条件是这个数的末两位数能被 4 整除.

3. 一个整数能被 5 整除的充分必要条件是这个数的个位数是 0 或 5.

4. 一个整数能被 3 整除的充分必要条件是这个数的各位数码之和能被 3 整除.

5. 一个整数能被 9 整除的充分必要条件是这个数的各位数码之和能被 9 整除.

6. 一个整数能被 11 整除的充分必要条件是这个数的奇位数码之和与偶位数码之和的差能被 11 整除.

7. 一个整数能被 $10n-1$（n 为自然数）整除的充分必要条件是把这个数的个位数截去以后，再加上这个个位数的 n 倍，它的和能被 $10n-1$ 整除.

即把 A 写成 $A=10x+y$，$y\in\{0, 1, 2, \cdots, 9\}$，则

$10n-1 \mid A \Leftrightarrow 10n-1 \mid x+ny$.

由此可判断整数 A 能否被 9，19，29，39，…整除.

8. 一个整数能被 $10n+1$（n 为自然数）整除的充分必要条件是把这个数的个位数截去之后，再减去这个个位数的 n 倍，它的差能被 $10n+1$ 整除.

即把 A 写成 $A=10x+y$，$y\in\{0, 1, 2, \cdots, 9\}$，则

$10n-1 \mid A \Leftrightarrow 10n+1 \mid x-ny$.

由此可判断整数 A 能否被 11，21，31，41，…整除.

【典型例题与基本方法】

例 1　（第 21 届意大利数学奥林匹克题）证明：任意 18 个连续的且小于或等于 2005 的正整数中，至少存在一个整数能被其各位数字之和整除.

证明　可证明这连续的 18 个数中一定有两个数是 9 的倍数，且它们的各位数字之和能被 9 整除.

由于小于或等于 2005 的正整数的各位数字之和最大是 28，所以，这两个数的各位数字之和只可能是 9，18 或 27.

若这两个数中有一个其各位数字之和为 9，命题显然成立.

若这两个数中有一个其各位数字之和为 27，则只可能是 999 或 1998 或 1989 或 1899，前两数均可以被 27 整除；若为 1989，则 1980 或 1998 满足条件；若为 1899，则 1890 或 1908 满足条件.

若这两个数各位数字之和均为 18，则这两个数一定有一个是偶数，这个数能被 18 整除.

例 2 有七块分别标有数码 1，2，3，4，5，6，7 的记分牌. 证明：由这七块记分牌组成的任何两个七位数中，一个都不能被另一个整除.

证明 设这七位数为$\overline{a_1a_2\cdots a_7}$.

由于 $a_1+a_2+\cdots+a_7=1+2+\cdots+7=28$，被 9 除余 1，则由这七个数码组成的七位数被 9 除余 1.

设 A，B 是其中的两个不同的七位数，且 A 能被 B 整除，则$\frac{A}{B}$是整数.

从而$\frac{A-B}{B}$是整数.

又 A 与 B 对模 9 余 1，则 $A-B$ 能被 9 整除，而 B 不能被 9 整除，于是$\frac{A-B}{B}$能被 9 整除.

又 $\frac{A-B}{B}<7$，则

$A-B=0$，即 $A=B$，与 A 和 B 不同矛盾.

例 3 （1963 年基辅数学奥林匹克题）如果在多位数 $\overline{3※4※1※0※8※2※40923※0※320※2※56}$中星号所在的数字是 0，1，2，3，4，5，6，7，8，9 的某一个排列（这些数中每个都用一次），那么所得的数能被 396 整除. 试证之.

证明 注意到 $396=4\cdot9\cdot11$.

由于已知的多位数的末两位数是 56，它能被 4 整除，所以这个多位数能被 4 整除.

再考虑这个多位数的数码之和，它是该数中已知的数码之和加上星号所表示的数码之和，这个和为

$(3+4+1+0+8+2+4+0+9+2+3+0+3+2+0+2+5+6)+$

$(0+1+2+3+4+5+6+7+8+9)=99$，

因此这个多位数能被 9 整除.

再考虑这个多位数的奇数位之和与偶数位之和.

奇数位之和：

$3+4+1+0+8+2+4+9+3+0+3+0+2+5=44.$

偶数位之和：

$0+1+2+3+4+5+6+7+8+9+0+2+2+6=55.$

由于这个多位数的偶数位之和与奇数位之和的差为 11，所以这个多位数能被 11 整除.

又因为 4，9，11 两两互素，所以这个多位数能被 $4\cdot 9\cdot 11=396$ 整除.

例 4 （2005 年罗马利亚数学奥林匹克题）证明：对每一个正整数 n，在十进制表示下，存在唯一的 n 位正整数能被 5^n 整除，其每一位数字都属于 {1，2，3，4，5}.

证明 用数学归纳法证明.

对每个正整数 n，存在一个唯一的 n 位数 A_n，能被 5^n 整除，其数字均属于集合 {1,2,3,4,5}.

显然：$A_1=5$，$A_2=25$.

假设 A_n 已定，设 $B_n=\frac{A_n}{5^n}$，则 $n+1$ 位数字 $\overline{c_{n+1}c_n\cdots c_1}=c_{n+1}10^n+\overline{c_nc_{n-1}\cdots c_1}$ 能被 5^n 整除，当且仅当 $\overline{c_nc_{n-1}\cdots c_1}$ 能被 5^n 整除.

由归纳假设得

$\overline{c_nc_{n-1}\cdots c_1}=A_n=5^nB_n$.

因此，$\overline{c_{n+1}c_n\cdots c_1}=5^n(2^nc_{n+1}+B_n)$.

当且仅当 $2^nc_{n+1}+B_n$ 能被 5 整除时，该数能被 5^{n+1} 整除.

因为 $(2^n,5)=1$，所以，$2^nx+b\equiv 0 \pmod 5$ 在集合 {1,2,3,4,5} 中有唯一解，其中 $n\in \mathbf{N}_+$，$b\in \mathbf{N}$.

例 5 （2007 年克罗地亚数学竞赛题）已知数列 $\{a_n\}$，$\{b_n\}$ 满足

$a_n=2^{2n+1}-2^{n+1}+1$，$b_n=2^{2n+1}+2^{n+1}+1$.

证明：对任意正整数 n，a_n、b_n 中有且仅有一个被 5 整除.

证明 先来证：对任意的 n，a_n 与 b_n 之积被 5 整除.

$$\begin{aligned}a_nb_n&=[(2^{2n+1}+1)-2^{n+1}][(2^{2n+1}+1)+2^{n+1}]\\&=(2^{2n+1}+1)^2-(2^{n+1})^2\\&=2^{4n+2}+2\times 2^{2n+1}+1-2^{2n+2}\\&=4^{2n+1}+1\\&=(4+1)(4^{2n}-4^{2n-1}+4^{2n-2}-\cdots-4+1)\\&=5(4^{2n}-4^{2n-1}+4^{2n-2}-\cdots-4+1).\end{aligned}$$

显然，$5|a_nb_n$.

再证：a_n、b_n 不能同时被 5 整除.

若 a_n、b_n 同时被 5 整除，则

$5|(b_n-a_n)$.

又 $b_n-a_n=2\times2^{n+1}=2^{n+2}$，$5\nmid 2^{n+2}$，矛盾.

综上，由于 5 是素数，a_n，b_n 中有且仅有一个被 5 整除.

例 6 （2005 年克罗地亚数学竞赛题）证明：在每个由 11 个正整数组成的集合中，有 6 个数的和能被 6 整除.

证明 先证明两个引理.

引理 1 在每个由 3 个正整数组成的集合中，存在 2 个数的和能被 2 整除.

引理 1 的证明：在每个由 3 个数组成的集合中，有 2 个数奇偶性相同，因此，其和为偶数.

引理 2 在每个由 5 个正整数组成的集合中，存在 3 个数的和能被 3 整除.

引理 2 的证明：如果存在 3 个数，被 3 除得到不同的余数，则它们的和能被 3 整除. 如果不存在这样的数，即它们中有 3 个数被 3 除时有相同的余数，则这 3 个数的和能被 3 整除.

下面证明原题.

运用引理 1 五次，能在所给的由 11 个正整数组成的集合中找到 5 对数的和为偶数. 对这 5 个和运用引理 2，知其中 3 个的和能被 3 整除. 所以，存在 6 个数满足其和能被 6 整除.

【解题思维策略分析】

1. 运用整数的可除性特征讨论整除问题

例 7 （1975 年基辅数学奥林匹克题）两人一起写一个由 1，2，3，4，5 这五个数码组成的 $2k$ 位数，第一个人写第一位数码，第二个人写第二位数码，第三位数码仍由第一个人写，依此类推. 在第一个人设法干扰的情况下，第二个人能否使所得之数被 9 整除？讨论以下两种情况：

(1) $k=10$.

(2) $k=15$.

解 设所写的 $2k$ 位数为 $N=\overline{a_1a_2\cdots a_{2k-1}a_{2k}}$，其中 $a_i\in\{1,2,3,4,5\}$.

设第一个人为 A，第二个人为 B.

奇数下标 i 的数码 a_i 由 A 选取，而偶数下标 i 的数码 a_i 由 B 选取.

再设 $S_i=\sum\limits_{j=1}^{i}a_j$.

则 N 能被 9 整除的充要条件是 S_{2k} 能被 9 整除.

(1) 当 $k=3m$（m 为自然数）时，我们可以证明，在这种情况下，不管 A 如何选取，B 总能获胜.

为此，对应 A 取的任意数 a_{2i-1}，$1\leqslant i\leqslant k$，B 应取 $a_{2i}=6-a_{2i-1}$，显然，由 $a_{2i-1}\in\{1,2,3,4,5\}$，可得 $6-a_{2i-1}=a_{2i}\in\{1,2,3,4,5\}$.

这时，对任意的 $i\leqslant k$，

$S_{2i}=(a_1+a_2)+\cdots+(a_{2i-1}+a_{2i})=6i.$

$S_{2k}=6k=18m.$

所以不管 A 如何选取，B 总能使 N 能被 9 整除.

(2) 当 k 不能被 3 整除时，我们证明，在这种情况下，A 可以使 B 不能达到目的.

为此，A 只要取 $a_1=3$，然后对应 B 取的任意 a_{2i}，$1\leqslant i\leqslant k-1$，$A$ 只要选取 $a_{2i+1}=6-a_{2i}$，这样一来

$$\begin{aligned}S_{2k}&=a_1+(a_2+a_3)+\cdots+(a_{2k-2}+a_{2k-1})+a_{2k}\\&=3+6(k-1)+a_{2k}\\&=6k-3+a_{2k}.\end{aligned}$$

如果 $k=3m+1$，那么

$S_{2k}=18m+3+a_{2k}.$

它被 9 除的余数为 $3+a_{2k}$，由 $a_{2k}\in\{1,2,3,4,5\}$，则

$3+a_{2k}\in\{4,5,6,7,8\}.$

此时 $S_{2k}\equiv4,5,6,7,8\pmod 9$.

因此，S_{2k} 不能被 9 整除.

如果 $k=3m+2$，那么

$S_{2k}=18m+9+a_{2k}.$

由于 $a_{2k}\in\{1,2,3,4,5\}$，则

$S_{2k}\equiv1,2,3,4,5\pmod 9$.

因此，S_{2k} 不能被 9 整除.

这样，当 k 不能被 3 整除时，A 可以采取上述策略使 B 不能达到目的.

例 8 （CMO-22 试题）试求不小于 9 的最小正整数 n，满足：对任给的 n 个整数（可以相同）a_1，a_2，…，a_n，总存在 9 个数 a_{i_1}，a_{i_2}，…，a_{i_9} $(1\leqslant i_1<i_2<\cdots<i_9\leqslant n)$ 及 $b_i\in\{4,7\}$ $(i=1,2,\cdots,9)$，使得 $b_1a_{i_1}+b_2a_{i_2}+\cdots+b_9a_{i_9}$ 为 9 的倍数.

解 取 $a_1=a_2=1$，$a_3=a_4=3$，$a_5=\cdots=a_{12}=0$，则其中任 9 个数均不满足要求，因 $n\geqslant13$. 下证 $n=13$ 可以. 为此，只要证明如果 m 个整数（可以相同）a_1，

a_2，…，a_m 中，不存在 3 个数 a_{i_1}，a_{i_2}，a_{i_3} 及 $b_1,b_2,b_3\in\{4,7\}$，使得 $b_1a_{i_1}+b_2a_{i_2}+b_3a_{i_3}$ 为 9 的倍数，则 $m\leqslant 6$ 或者 $7\leqslant m\leqslant 8$ 且 a_1，a_2，…，a_m 中有 6 个 a_{i_1}，a_{i_2}，…，a_{i_6} 及 b_1，b_2，…，$b_6\in\{4,7\}$使得 $9|b_1a_{i_1}+b_2a_{i_2}+\cdots+b_6a_{i_6}$.

设

$A_1=\{i|1\leqslant i\leqslant m,9|a_i\}$，

$A_2=\{i|1\leqslant i\leqslant m,a_i\equiv 3(\text{mod }9)\}$，

$A_3=\{i|1\leqslant i\leqslant m,a_i\equiv 6(\text{mod }9)\}$，

$A_4=\{i|1\leqslant i\leqslant m,a_i\equiv 1(\text{mod }3)\}$，

$A_5=\{i|1\leqslant i\leqslant m,a_i\equiv 2(\text{mod }3)\}$，

则$|A_1|+|A_2|+|A_3|+|A_4|+|A_5|=m$，且

(1) 若 $i\in A_2$，$j\in A_3$，则 $9|4a_i+4a_j$；

(2) 若 $i\in A_4$，$j\in A_5$，则 9 能整除 $4a_i+4a_j$，$4a_i+7a_j$，$7a_i+4a_j$ 之一. 这是因为 $4a_i+4a_j$，$4a_i+7a_j$，$7a_i+4a_j$ 均是 3 的倍数且模 9 两两不同余；

(3) 若 i，j，$k\in A_2$ 或者 i，j，$k\in A_3$，则 $9\mid 4a_i+4a_j+4a_k$；

(4) 若 i，j，$k\in A_4$ 或者 i，j，$k\in A_5$，则 9 能整除 $4a_i+4a_j+4a_k$，$4a_i+4a_j+7a_k$，$4a_i+7a_j+7a_k$ 之一. 这是因为这三个数均是 3 的倍数且模 9 两两不同余.

由假设，有$|A_i|\leqslant 2(1\leqslant i\leqslant 5)$.

若$|A_1|\geqslant 1$，则$|A_2|+|A_3|\leqslant 2$，$|A_4|+|A_5|\leqslant 2$. 这样 $m=|A_1|+|A_2|+|A_3|+|A_4|+|A_5|\leqslant 6$.

下设$|A_1|=0$，$m\geqslant 7$，此时 $7\leqslant m=|A_1|+|A_2|+|A_3|+|A_4|+|A_5|\leqslant 8$.

因此

$\min\{|A_2|,|A_3|\}+\min\{|A_4|,|A_5|\}\geqslant 3$.

由 (1) 和 (2) 知，存在 i_1，i_2，…，$i_6\in A_2\cup A_3\cup A_4\cup A_5$，$i_1<i_2<\cdots<i_6$ 及 b_1，b_2，…，$b_6\in\{4,7\}$使 $9|b_1a_{i_1}+b_2a_{i_2}+\cdots+b_6a_{i_6}$.

综上所述，所求的最小的 $n=13$.

例 9 （第 30 届俄罗斯数学奥林匹克题）在 100×100 方格表的每个方格中均填写着 1 个非 0 数码. 已知沿着各行填写的 100 个 100 位数均可被 11 整除. 试问：在沿着各列填写的 100 个 100 位数中是否可能恰好有 99 个可被 11 整除?

解 不可能.

假设可能. 我们知道，一个正整数可被 11 整除，当且仅当它的偶数位上的数字之和与奇数位上的数字之和被 11 除的余数相等.

现在，按照国际象棋棋盘的染色规则，将各个小方格交替地染为黑色与白色. 于是，由题意知每一行中，黑色方格中的数码之和都与白色方格中的数码之和被 11

除的余数相等，即所有黑色方格中的数码之和与所有白色方格中的数码之和被 11 除的余数相等.

如果有 99 列中的 100 位数可被 11 整除，那么，这 99 列中的黑色方格中的数码之和都与白色方格中的数码之和被 11 除的余数相等，而剩下的一列中的黑色方格中的数码之和也是与白色方格中的数码之和被 11 除的余数相等. 从而，该列中的 100 位数也能被 11 整除.

例 10 （2003—2004 年度德国数学竞赛题）已知 p，q 是互素的正整数，且 $p\neq q$. 将正整数集分成三个子集 A，B，C，使得对于每个正整数 z，这三个子集中的每一个恰各包含 z，$z+p$，$z+q$ 这三个整数之一. 证明：存在这样的分拆，当且仅当 $p+q$ 能被 3 整除.

证明 充分性.

设 $p+q$ 可以被 3 整除，假设

$p\equiv1\pmod 3$，$q\equiv2\pmod 3$.

定义 $A=\{a\in\mathbf{N}_+\mid a\equiv0\pmod 3\}$，

$B=\{b\in\mathbf{N}_+\mid b\equiv1\pmod 3\}$，

$C=\{c\in\mathbf{N}_+\mid c\equiv2\pmod 3\}$.

容易验证 z，$z+p$，$z+q$ 分别属于这三个不同的子集，所以，这三个子集满足条件.

必要性.

设存在一种分拆，且假设

$z\in A$，$z+p\in B$，$z+q\in C$.

由于 $(z+p)+q\notin B$，$(z+q)+p\notin C$，所以，

$z+p+q\in A$.

于是，如果 $z_1\equiv z_2\pmod{p+q}$，则 z_1 和 z_2 属于同一个子集.

闭区间 $I=[0,p+q-1]$ 中包含 $p+q$ 个不同的整数，模 $p+q$ 的剩余类只对应着 I 中的一个整数.

下面证明：I 中的整数分别属于 A，B，C 的数目相等，即一定有 $p+q$ 可以被 3 整除.

对于每一个 $z\in A\cap I$，定义 $p(z)$ 为 $z+p$ 模 $p+q$ 的余数，$q(z)$ 为 $z+q$ 模 $p+q$ 的余数. 显然 $p(z)\notin A$，$q(z)\notin A$. 而且，对于所有 $z,z_1,z_2\in A\cap I$，我们有 $p(z)\neq q(z)$. 当 $z_1\neq z_2$ 时，$p(z_1)\neq p(z_2)$，$q(z_1)\neq q(z_2)$. 若存在 z_1,z_2，使得 $p(z_1)=q(z_2)$，则 $p(z_1)-q=q(z_2)-q\in A$. 于是，

$z_1+2p=p(z_1)-q+(p+q)\in A$.

另一方面，$(z_1+p)+q\in A$，所以，$z_1+p\notin A$，同时$(z_1+p)+p=z_1+2p\notin A$，矛盾.

因此，集合 $I\cap(B\cup C)$中元素的数目至少是集合 $I\cap A$ 中元素数目的两倍.

故 $p+q=|I|=|A\cap I|+|(B\cup C)\cap I|\geqslant 3|A\cap I|$.

类似地，$p+q\geqslant 3|B\cap I|$，$p+q\geqslant 3|C\cap I|$.

但 $p+q=|A\cap I|+|B\cap I|+|C\cap I|$，所以，

$A\cap I|=|B\cap I|=|C\cap I|$.

于是，$p+q=3|A\cap I|$.

例 11 判断一个正整数能否被 7 整除，可采用“割尾法”，如对 2527 割掉末位数码 7 得到 252，再从 252 中减去被割掉的末位数码 7 的 2 倍得到 238，这称为一次“割尾”，对 238 再进行一次“割尾”得到 7，显然 7 是 7 的倍数，从而 2527 可被 7 整除.

试证明一个正整数能被 7 整除的充分必要条件是对该数进行有限次“割尾”所得到的数能被 7 整除.

证法 1 设正整数为 $A=\overline{a_{n-1}a_{n-2}\cdots a_1a_0}$，即

$$A=10^{n-1}a_{n-1}+10^{n-2}a_{n-2}+\cdots+10a_1+a_0=\sum_{i=0}^{n-1}a_i\cdot 10^i.$$

经过一次“割尾”后，A 变为

$$A'=\sum_{i=1}^{n-1}a_i\cdot 10^{i-1}-2a_0,$$

显然有

$$10A'=A-21a_0.$$

由 $(7,10)=1$ 知，若 $7|A$，必有 $7|A'$.

反之，若 $7|A'$，必有 $7|A$.

从而本题得证.

证法 2 设正整数为 $A=\overline{a_na_{n-1}\cdots a_2a_1}$，则

$$\begin{aligned}5A&=5\cdot\overline{a_na_{n-1}\cdots a_2a_1}\\&=5\cdot(\overline{a_na_{n-1}\cdots a_2}\cdot 10+a_1)\\&=5\cdot(9\cdot\overline{a_na_{n-1}\cdots a_2}+3a_1)+5\cdot(\overline{a_na_{n-1}\cdots a_2}-2a_1)\\&\equiv 5\cdot(2\cdot\overline{a_na_{n-1}\cdots a_2}-4a_1)+5\cdot(\overline{a_na_{n-1}\cdots a_2}-2a_1)\\&\equiv 10\cdot(\overline{a_na_{n-1}\cdots a_2}-2a_1)+5\cdot(\overline{a_na_{n-1}\cdots a_2}-2a_1)\\&=15\cdot(\overline{a_na_{n-1}\cdots a_2}-2a_1)\\&\equiv\overline{a_na_{n-1}\cdots a_2}-2a_1\pmod 7.\end{aligned}$$

因此，当 $7|A$ 时，有

$5A\equiv 0 \pmod 7$，从而

$\overline{a_na_{n-1}\cdots a_2}-2a_1\equiv 0 \pmod 7$.

于是 $7|\overline{a_na_{n-1}\cdots a_2}-2a_1$.

反之，若 $7|\overline{a_na_{n-1}\cdots a_2}-2a_1$，则 $7|5A$，再由 $(5,7)=1$ 可得 $7|A$.

于是本题得证.

例 12 （1965 年第 28 届莫斯科数学奥林匹克题）试证对 37 的整除性的下述特征：为了判断一个整数能否被 37 整除，可以将它自右向左分为小节，每一小节三个数码，如果所得的这些三位数之和可被 37 整除，那么原来的数就可被 37 整除（这里所说的“三位数”是广义的，因为有些小节可能以 0 开头，因此在事实上是两位数或一位数，而当原来的数的位数不能被 3 整除时，最左边的小节也不是三位数）.

证明 我们以九位数 $A=\overline{abcdefghi}$ 为例，对于任意 n 位数的证法完全相同.

本题等价于 A 能被 37 整除的充要条件是 $\overline{abc}+\overline{def}+\overline{ghi}$ 能被 37 整除.

事实上，

$$\begin{aligned}A&=\overline{abcdefghi}=\overline{abc}\cdot 10^6+\overline{def}\cdot 10^3+\overline{ghi}\\&=\overline{abc}\cdot 999999+\overline{def}\cdot 999+(\overline{abc}+\overline{def}+\overline{ghi}).\end{aligned}$$

由于 999999 和 999 能被 37 整除，所以，当且仅当 $37|\overline{abc}+\overline{def}+\overline{ghi}$ 时，$37|A$.

例 13 （第 18 届爱尔兰数学奥林匹克题）已知 x 是一个整数，y，z，w 是奇数. 证明：17 能整除 $x^{y^{z^w}}-x^{y^z}$.

证明 先证明一个引理.

引理 设 n 是奇数，则 $n^4\equiv 1 \pmod{16}$.

引理的证明：注意到

$$\begin{aligned}(4k+1)^4&=256k^4+256k^3+96k^2+16k+1\\&\equiv 1 \pmod{16},\\(4k+3)^4&=256k^4+768k^3+864k^2+432k+81\\&\equiv 1 \pmod{16}.\end{aligned}$$

所以，引理成立.

下面证明原题.

因为 z,w 是奇数，所以，

$z^w=z(z^2)^{\frac{w-1}{2}}\equiv z \pmod 4$.

由引理得 $y^4\equiv 1 \pmod{16}$.

故 $y^{z^w}=y^z(y^4)^{\frac{z^w-z}{4}}\equiv y^z \pmod{16}$.

若 $17|x$，显然 $17|(x^{y^{z^w}}-x^{y^z})$；

若 $17\nmid x$，由费马小定理得 $x^{16}\equiv1 \pmod{17}$，则

$$x^{y^{z^w}}=x^{y^z}(x^{16})^{\frac{y^{z^w}-y^z}{16}}\equiv x^{y^z} \pmod{17}.$$

所以，$17|(x^{y^{z^w}}-x^{y^z})$.

例 14 （*1956 年基辅数学奥林匹克题*）圆上有 1956 个数码，已知从某一位起把这些数按顺时针方向记下，得到的一个 1956 位数能被 27 整除．证明如果从任何一位起把这些数码按顺时针方向记下的话，那么所得的一个 1956 位数也能被 27 整除．

证明 本题的结论对于圆上写 $3n$ 个数码也是成立的．现在我们证明这个一般情形．

假定从某一位开始按顺时针方向读起，得到的 $3n$ 位数为

$$\overline{a_1a_2\cdots a_{3n}}=10^{3n-1}a_1+10^{3n-2}a_2+\cdots+10_{a_{3n-1}}+a_{3n}.$$

并设 $27\mid\overline{a_1a_2\cdots a_{3n}}$.

我们只要证明从相邻一位读起所得到的数 $\overline{a_2a_3\cdots a_{3n}a_1}$ 也能被 27 整除即可．

研究下面的差：

$$10\cdot\overline{a_1a_2a_3\cdots a_{3n}}-\overline{a_2a_3\cdots a_{3n}a_1}=(10^{3n}-1)a_1=(1000^n-1)a_1.$$

由于 $1000\equiv1 \pmod{27}$，则

$$1000^n\equiv1 \pmod{27}, 27|1000^n-1.$$

又 $27|10\cdot\overline{a_1a_2\cdots a_{3n}}$，所以

$$27|\overline{a_2a_3\cdots a_{3n}a_1}.$$

例 15 （*1984 年第 16 届加拿大数学竞赛题*）如果一个整数满足：

(1)它的各位数字都不为 0；

(2)它可以被它的各位数字和整除．

就称该整数可被其数字和整除(例如 322 可被其数字和整除)．

证明有无限多个可被其数字和整除的整数．

证明 事实上，对于任何自然数 n，数 $\underbrace{11\cdots1}_{3^n\text{个}}$ 都是这样的整数，而这样的整数有无限多个．

下面用数学归纳法给予证明．

(1) $n=1$ 时，111 可被其数字和 $1+1+1=3$ 整除，结论成立；

(2)假设 $n=k$ 时，数 $\underbrace{11\cdots1}_{3^k\text{个}}$ 可被其数字和 3^k 整除．

那么当 $n=k+1$ 时，由于



$$\underbrace{11\cdots1}_{3^{k+1}个}=\underbrace{100\cdots0}_{3^k位}\underbrace{100\cdots1}_{3^k位}\cdot\underbrace{11\cdots1}_{3^k个}.$$

它的第一个因数的数字和是 3，因而能被 3 整除，第二个因数由归纳假设能被 3^k 整除，所以这两个因数的乘积可被 3^{k+1} 整除.

从而 $n=k+1$ 时结论成立.

于是对所有的 $n\in\mathbf{N}$，结论成立.

例 16 （2005 年俄罗斯数学奥林匹克题）在一个由正整数构成的等差数列 a_1，a_2，…中，对每个 n，乘积 a_na_{n+31} 都能被 2005 整除. 试问：能否断言“数列中的每一项都能被 2005 整除”？

解 可以断言.

设数列的公差为 d.

若对每个 n，都有 $5\mid a_{n+31}$，则易知 $5\mid d$.

若存在某个 n，使得 $5\nmid a_{n+31}$，则 $5\mid a_n$，$5\mid a_{n+62}$，于是，$5\mid(a_{n+62}-a_n)=62d$.

由于 62 与 5 互素，所以，$5\mid d$.

总之，在一切情况下，都有 $5\mid d$.

因此，$5\mid(a_na_{n+31}-31a_nd)=a_n^2$.

由于 5 是素数，所以，$5\mid a_n$.

注意到 401 也是素数，经过类似推理可知，对每个 n，都有 $401\mid a_n$.

由于 5 与 401 互素，所以，对每个 n，a_n 都能被 $5\times401=2005$ 整除.

2. 运用整数的可除性特征求某些数位上的数字

例 17 （1980 年第 12 届加拿大数学竞赛题）设 $\overline{a679b}$ 是一个十进制的五位数，可被 72 整除，试决定 a 与 b 的值.

解 由于 $72=8\cdot9$，8 和 9 互素.

所以 $\overline{a679b}$ 若能被 72 整除，则必须同时能被 8 和 9 整除.

如果 $\overline{a679b}$ 能被 8 整除，其充要条件是末三位 $79b$ 能被 8 整除.

由此可得到唯一的 $b=2$.

如果 $\overline{a6792}$ 能被 9 整除，其充要条件是它的各位数字和能被 9 整除，即

$$a+6+7+9+2=24+a$$

能被 9 整除，可得到唯一的 $a=3$.

于是 $a=3$，$b=2$，此时 $36972=72\cdot511$.

例 18 （上海市数学竞赛题）设自然数 $\overline{62\alpha\beta427}$ 为 99 的倍数，求 α，β.

解 因为 $\overline{62\alpha\beta427}$ 是 99 的倍数，所以它既是 9 的倍数，又是 11 的倍数.

因为 $\overline{62\alpha\beta427}$ 是 9 的倍数，则

$6+2+\alpha+\beta+4+2+7=9m\ (m\in\mathbf{N})$，即

$\alpha+\beta+3=9(m-2)$.

因为 $0\leqslant\alpha\leqslant9$，$0\leqslant\beta\leqslant9$，所以

$3\leqslant\alpha+\beta+3\leqslant21$.

于是 $\alpha+\beta+3=9$ 或 $\alpha+\beta+3=18$，即

$\alpha+\beta=6$ 或 $\alpha+\beta=15$.

因为$\overline{62\alpha\beta427}$是 11 的倍数，则

$(6+\alpha+4+7)-(2+\beta+2)=11k\ (k\in\mathbf{Z}^{-})$，即

$\alpha-\beta+13=11k$.

因为 $4\leqslant\alpha-\beta+13\leqslant22$，所以

$\alpha-\beta+13=11$ 或 $\alpha-\beta+13=22$，即

$\alpha-\beta=-2$ 或 $\alpha-\beta=9$.

从而可以得到四个方程组

$\begin{cases}\alpha+\beta=6,\\\alpha-\beta=-2,\end{cases}$ $\begin{cases}\alpha+\beta=6,\\\alpha-\beta=9,\end{cases}$ $\begin{cases}\alpha+\beta=15,\\\alpha-\beta=-2,\end{cases}$ $\begin{cases}\alpha+\beta=15,\\\alpha-\beta=9.\end{cases}$

解以上方程组，由于两数的和与差有相同的奇偶性，并且 $0\leqslant\alpha\leqslant9$，$0\leqslant\beta\leqslant9$，所以只有解 $\alpha=2$，$\beta=4$.

例 19 （*2005 年克罗地亚数学竞赛题*）求所有可用十进制表示$\overline{13xy45z}$，且能被 792 整除的正整数，其中，x，y，z 为未知数.

解 因为 $792=8\times9\times11$，所以，数字$\overline{13xy45z}$能被 8，9，11 整除.

由 $8\mid\overline{13xy45z}$，知 $8\mid\overline{45z}$.

而$\overline{45z}=450+z=448+(z+2)$，因此，

$8\mid(z+2)$.

故 $z=6$.

由 $9\mid\overline{13xy456}$，知

$9\mid(1+3+x+y+4+5+6)$.

而 $1+3+x+y+4+5+6=x+y+19=18+(x+y+1)$，

因此，$9\mid(x+y+1)$.

故 $x+y=8$ 或 $x+y=17$.

由 $11\mid\overline{13xy456}$，知

$11\mid(6-5+4-y+x-3+1)$.

而 $6-5+4-y+x-3+1=x-y+3$，因此，

$x-y=-3$ 或 $x-y=8$.

此时，有两种可能：

(1) 若 $x+y$ 为偶数，则 $x+y=8$ 且 $x-y=8$. 从而，$x=8$，$y=0$.

(2) 若 $x+y$ 为奇数，则 $x+y=17$ 且 $x-y=-3$. 从而，$x=7$，$y=10$，不可能.

所以，唯一的正整数为 1380456.

例 20 （2003 年加拿大数学奥林匹克题）求 $2003^{2002^{2001}}$ 的末三位数字.

解
$$\begin{aligned}2003^{2002^{2001}}&\equiv 3^{2002^{2001}}\pmod{10^3}\\&=9^{2^{2000}\times 1001^{2001}}\\&=(10-1)^k\text{（令 }k=2^{2000}\times 1001^{2001}\text{）}\\&\equiv C_k^2\times 10^2-k\times 10+1\pmod{10^3}.\end{aligned}$$

其中
$$\begin{aligned}k&=2^{2000}\times 1001^{2001}\equiv 2^{2000}=1024^{200}\\&\equiv 24^{200}=3^{200}\times 2^{600}\equiv 3^{200}\times 24^{60}=3^{260}\times 2^{180}\\&\equiv 3^{260}\times 24^{18}=3^{278}\times 2^{54}\\&\equiv 3^{278}\times 24^5\times 2^4=3^{283}\times 2^{19}\\&\equiv 3^{283}\times 24\times 2^9=3^{284}\times 2^{12}\\&\equiv 3^{284}\times 24\times 2^2=(10-1)^{142}\times 96\\&\equiv (C_{142}^2\times 10^2-142\times 10+1)\times 96\\&\equiv 681\times 96\equiv 376\pmod{10^3}.\end{aligned}$$

故
$$\begin{aligned}2003^{2002^{2001}}&\equiv C_{376}^2\times 10^2-376\times 10+1\\&\equiv 241\pmod{10^3}.\end{aligned}$$

例 21 设一个整数被某个数 $M(M\neq 1)$ 整除的判别法则不依赖于整数的各位数码的顺序，证明 M 等于 3 或 9.

证明 设 M 是 n 位数.

研究一切形如 $\overline{10a_1a_2\cdots a_n}$ 的 $n+2$ 位数.

因为数码 $a_1,a_2,\cdots,a_n$ 的每一个都可以彼此无关地取自 0 到 9 这 10 个不同的数码，因此，所要研究的数有 10^n 个连续的数.

由于 $10^n>M$，所以这些数中至少可找到一个数被 M 整除. 设这个数是 $\overline{10b_1b_2\cdots b_n}$，即 $M\mid\overline{10b_1b_2\cdots b_n}$.

由题设，被 M 整除的判别法则不依赖于数码的顺序，则

$M\mid\overline{b_1b_2\cdots b_n01}$，

$M\mid\overline{b_1b_2\cdots b_n10}$.

从而 M 也能整除它们的差，即

$M\mid\overline{b_1b_2\cdots b_n10}-\overline{b_1b_2\cdots b_n01}$，即 $M\mid 9$.

于是 $M=3,9$（因为$M\neq 1$）.

另一方面，被 3 和 9 整除的判别法则只需检验一个数的各位数码之和而与各位数码的顺序无关.

所以$M=3$或 9.

例 22 （1989 年第 21 届加拿大数学竞赛题）定义$\{a_n\}_{n=1}^{\infty}$如下：

$a_1=1989^{1989}$，且$a_n(n>1)$等于a_{n-1}的各位数字之和，a_5等于多少？

解 由于$a_1=1989^{1989}<10000^{1989}$，

而10000^{1989}共有$4\cdot 1989+1=7957$位.

所以a_1不多于 7957 位.

由题设，a_2是a_1的各位数字之和，则

$a_2<10\cdot 8000=80000$.

所以a_2最多为 5 位数，因而

$a_3\leqslant 7+4\cdot 9=43$，$a_4\leqslant 4+9=13$.

于是a_5为一位数.

由于任何一个正整数能被 9 整除的充要条件是它的数字和能被 9 整除.

由于$9|1+9+8+9=27$，则$9|1989^{1989}$.

于是 9 a_5.

即$a_5=0$或 9.

$a_5=0$显然不可能，所以$a_5=9$.

3. 运用整数的可除性特征求某些整数

例 23 （1979 年广西壮族自治区数学竞赛题）由数字 0，1，2，3，4，5 能否组成数字不重复且能被 11 整除的六位数？为什么？

解 设所组成的六位数是$\overline{a_1a_2a_3a_4a_5a_6}$. 若这个六位数能被 11 整除，则

$a_1-a_2+a_3-a_4+a_5-a_6=11n$，即

$a_1+a_2+a_3+a_4+a_5+a_6=11n+2(a_2+a_4+a_6)$. ①

由于$a_1+a_2+a_3+a_4+a_5+a_6=15$，则

$11n+2(a_2+a_4+a_6)=15$. ②

显然，$0\leqslant n<2$，从而$n=0$或$n=1$.

(1) 当$n=0$时，②化为

$2(a_2+a_4+a_6)=15$，

此式左端为偶数，右端为奇数，不可能成立.

(2) 当$n=1$时，②化为

$a_2+a_4+a_6-2$，

但是，0，1，2，3，4，5 中任意三个数之和都大于 2，所以此时也无解.

综合以上，由 0，1，2，3，4，5 不可能组成数字不重复且能被 11 整除的六位数.

例 24 （第 48 届斯洛文尼亚数学奥林匹克题）求所有的五位数$\overline{abcde}$，该数能被 9 整除，且$\overline{ace}-\overline{bda}=760$.

解 方程$\overline{ace}-\overline{bda}=760$ 可以改写为

$100a+10c+e-100b-10d-a=760$，

由此可得 $e=a$.

将方程两边除以 10，可得

$10(a-b)+(c-d)=76$.

因此，只有两种可能

$c-d=6$ 或 $c-d=-4$.

如果 $c-d=6$，则有

$c=d+6$，$a=b+7$.

由于五位数能被 9 整除，因此，

$$\begin{aligned}a+b+c+d+e&=b+7+b+d+6+d+b+7\\&=3b+2d+20=3b+2(d+1+9)\end{aligned}$$

能被 9 整除.

所以，$d+1$ 能被 3 整除.

由于 $c-d=6$，可得 $d=2$，于是，$c=8$.

同时，$3(b+2)$能被 9 整除.

由于 $a=b+7$，故有 $b=1$.

这时，所求的五位数是 81828.

如果 $c-d=-4$，则有

$d=c+4$，$a=b+8$.

因此，$a=8$，$b=0$，或 $a=9$，$b=1$.

若 $a=8$，由

$9|(a+b+c+d+e)=8+2c+4+8$，

可导出，$2c+2$ 能被 9 整除.

于是，$c=8$，进而 $d=c+4=12$，不是一位数字.

若 $a=9$，由

$9|(a+b+c+d+e)=10+2c+4+9$，

可导出 $2c+5$ 能被 9 整除.

于是，$c=2$，相应的五位数是 91269.

例 25 （1987 年北京市数学竞赛题）$\overline{a_1a_2a_3\cdots a_{1999}a_{2000}}$ 是按如下规则写出的一个两千位的自然数（其中诸 a_i 代表阿拉伯数码）：先写出 a_1，接着依规则写 a_2，a_3，…，当 a_i 已写出，接着写 a_{i+1} 时，要使两位数 $\overline{a_ia_{i+1}}$ 是 17 或 23 的倍数（$i=1$，2，…，1999）．若按上述规则写出的一个两千位的自然数的各数码 a_i 中，1，9，8，7 这四个数码都出现过，求证写出的这个两千位自然数必定是合数.

证明 两位数中，17 的倍数有

17，34，51，68，85；

23 的倍数有

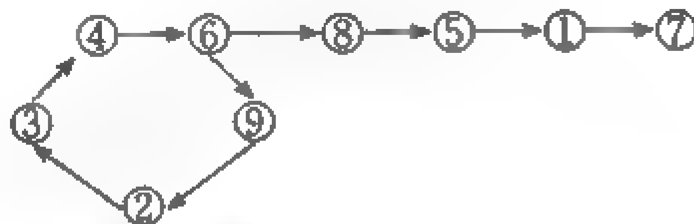
23，46，69，92.

以上 9 个数中，个位数里 1，2，3，4，5，6，7，8，9 均出现.

十位数中，6 出现两次，7 没出现，其余数字 1，2，3，4，5，8，9 均出现一次.

显然，7 不能作十位数，即 7 不能在两千位数的前 1999 位出现，即 7 是这个两千位数的最后一位.

这样，7 的前一位应是 1（17 是 17 的倍数），再前面应有 5 出现（51 是 17 的倍数），…，可排成下面一个图：



这样，某个数码出现，依图中箭头所指即下面出现的数码.

显然，在两千位数 $\overline{a_1a_2\cdots a_{1999}a_{2000}}$ 中，

$a_{2000}=7$，$a_{1999}=1$，$a_{1998}=5$，$a_{1997}=8$，$a_{1996}=6$，

从 1996 位开始的前 1996 位即从 $a_1\to a_{1996}=6$ 位都是在 $6\to9\to2\to3\to4\to6\to9\to\cdots$ 中循环，且每五个数为一个循环节.

所以这两千位数的所有数码之和为

$(6+9+2+3+4)\cdot399+(6+8+5+1+7)=24\cdot399+27=3\cdot(8\cdot399+9)$.

因此这个两千位数是 3 的倍数，当然是一个合数.

4．借助于整数的可除性特征处理问题

例 26 （第 30 届俄罗斯数学奥林匹克题）设 $\{N_1,\cdots,N_k\}$ 是由五位数（十进制）构成的数组，使得任何一个各位数字形成非降序列的五位数中都至少有一个数字与数 $N_1,\cdots,N_k$ 中的某个数的相同位置上的数字相同．试求 k 的最小可能值.

解 所求最小的值为 2. 理由如下：

具有所述性质的数组不可能仅由一个五位数构成. 事实上，对于任何一个五位数 $N=\overline{abcde}$，都存在不同于 a，b，c，d，e 的数码 g，从而，N 的任何一位数都不与 $G=\overline{ggggg}$ 相同.

下面证明：由数 $N_1=\overline{13579}$ 和 $N_2=\overline{12468}$ 所构成的数组即可满足题意.

任取一个五位数 $A=\overline{a_1a_2a_3a_4a_5}$，其中 $a_1\leqslant a_2\leqslant a_3\leqslant a_4\leqslant a_5$. 如果 A 的任何一位数都不与 N_1 和 N_2 的相同位置上的数字相同，那么，必有 $a_5\leqslant 7$，因此，$a_4\leqslant 7$. 但由于 a_4 既不同于 N_1 的十位数，又不同于 N_2 的十位数，因此，$a_4\leqslant 5$，故 $a_3\leqslant 5$. 又由于 a_3 既不同于 N_1 的百位数，也不同于 N_2 的百位数，因此，$a_3\leqslant 3$，故 $a_2\leqslant 3$. 如此下去，就又推出 $a_2\neq 3$，$a_2\neq 2$，于是，必有 $a_1=1$，从而，其首位数与 N_1（也与 N_2）的首位数相同.

例 27 （1986 年国家集训队选拔考试题）自然数 A 的十进制表示为 $\overline{a_na_{n-1}\cdots a_0}$，令 $f(A)=2^na_0+2^{n-1}a_1+\cdots+2a_{n-1}+a_n$，记 $A_1=f(A)$，$A_{i+1}=f(A_i)$ $(i=1,2,\cdots,n)$.

证明：(1) 必有自然数 k，使得 $A_{k+1}=A_k$.

(2) 若 $A=19^{86}$，问上述的 A_k 等于多少？并说明理由.

证明 (1) $n=0$ 时，对任意 k，有 $A_k=A$.

当 $n=1$ 时，显然有 $A\geqslant f(A)$.

当 $n\geqslant 2$ 时，

$$\begin{aligned}f(A)&=2^na_0+2^{n-1}a_1+\cdots+2a_{n-1}+a_0\\&\leqslant(2^n+2^{n-1}+\cdots+2+1)\cdot 9\\&=(2^{n+1}-1)\cdot 9.\end{aligned}$$

$$\begin{aligned}A&\geqslant 10^na_n\geqslant 10^n=10\cdot 10^{n-1}>9\cdot 10^{n-1}\\&>9\cdot 2^3\cdot 10^{n-2}\geqslant 9\cdot 2^3\cdot 2^{n-2}=9\cdot 2^{n+1}\\&>9(2^{n+1}-1)\geqslant f(A).\end{aligned}$$

从而 $n\geqslant 2$ 时有 $A>f(A)$.

这就意味着对 A 每进行一次操作，就变小一次，从而有

$A_1>A_2>A_3>\cdots$

因此必存在某个 $k\in\mathbf{N}$，使得

$A_k<100$.

若 A_k 为两位数，则可设 $A_k=\overline{ab}=10a+b$，则

$A_{k+1}=2b+a$，从而

$A_k-A_{k+1}=9a-b$.

显然，当 $a=1$，$b=9$ 时，$A_k=19$，而

$A_k-A_{k+1}=0$，即

$A_k=A_{k+1}$.

此时问题已得证.

若 $a\neq1$ 或 $b\neq9$，则 $9a-b>0$，即 $A_k>A_{k+1}$.

此时对 A_k 再进行一次操作，得到 A_{k+1}. 若 $A_{k+1}=19$，此时有 $A_{k+2}=A_{k+1}$，否则必可再经过某次操作得到一位数，记为 $A_t=a$. 于是有 $A_{t+1}=A_t$.

由以上，必存在自然数 k，使得 $A_{k+1}=A_k$.

(2) 首先证明，若 $10x+y$（x 为正整数，y 为非负整数）能被 19 整除，则 $x+2y$ 能被 19 整除.

这是因为

$10x+y=10(x+2y)-19y$.

而$(10,19)=1$.

若 $19|10x+y$,则 $19|x+2y$;反之，若 $19|x+2y$，则 $19|10x+y$.

因此,若 $19|A=\overline{a_na_{n-1}\cdots a_0}$,则

$19|\overline{a_na_{n-1}\cdots a_1}+2a_0$,

$19|\overline{a_na_{n-1}\cdots a_2}+2(a_1+2a_0)$.

如此下去，

$19|a_n+2a_{n-1}+\cdots+2^{n-1}a_1+2^na_0=f(A)$.

由于 $A=19^{86}$,则 $19|A$,于是 $19|A_1=f(A)$,进而

A_1，A_2，…都能被 19 整除.

又由 (1)，$A_1>A_2>\cdots>A_k$，则

$A_k=19$.

例 28 （2005 年英国数学奥林匹克题）确定由 7 个不同素数组成的等差数列中，最大项的最小可能值.

解 设等差数列为

p，$p+d$，$p+2d$，$p+3d$，$p+4d$，$p+5d$，$p+6d$.

易知，$p>2$. 因为若 $p=2$，则 $p+2d$ 为偶数且非 2，其不是素数.

因为 p 必为奇数，则 d 是偶数. 否则，$p+d$ 是偶数且大于 2，其不是素数.

又 $p>3$，因为若 $p=3$，则 $p+3d$ 是 3 的倍数且非 3，其不是素数.

所以，d 必须是 3 的倍数，否则，$p+d$ 和 $p+2d$ 中的一个将会是 3 的倍数.

用同样的方法，$p>5$，因为若 $p=5$，则 $p+5d$ 是 5 的倍数且非 5.

类似地，d 是 5 的倍数，否则 $p+d$，$p+2d$，$p+3d$，$p+4d$ 中的一个将会是 5 的倍数，其不是素数.

综上，有 $p\geqslant 7$ 和 $30\mid d$.

若 $p>7$，当 $7\nmid d$ 时，总有 7 的倍数存在于等差数列中，故 $7\mid d$. 这表示 $210\mid d$. 此时，最后项的最小可能值为 $11+6\times 210=1271$.

若 $p=7$（同时 $30\mid d$），则必须避免在数列中有 $187=11\times 17$. 因此，必须有 $d\geqslant 120$.

若 $d=120$，则数列为

7，127，247，367，487，607，727.

但 $247=13\times 19$，所以，这不成立.

当 $d=150$ 时，数列为

7，157，307，457，607，757，907，且所有的数为素数.

因为 $907<1271$，此即为最大项的最小可能值.

例 29 （第 55 届捷克和斯洛伐克数学奥林匹克题）正整数数列 $\{a_n\}$ 满足 $a_{n+1}=a_n+b_n$，$n\geqslant 1$，其中 b_n 是将 a_n 的各位数字的次序反过来得到的数（数 b_n 的首位数字可以是零）. 例如 $a_1=170$，$a_2=241$，$a_3=383$，$a_4=766$，等等. 问：a_7 是否可以是一个素数？

解 a_7 不能是素数.

证法 1 我们证明 a_7 总是一个能被 11 整除的合数.

若 $m=\overline{c_kc_{k-1}\cdots c_1c_0}$，则 m 除以 11 的余数与 $\text{res}(m)=c_0-c_1+c_2-\cdots+(-1)^kc_k$ 除以 11 的余数相同.

因此，$\text{res}(b_n)=\pm\text{res}(a_n)$，

其中，当 a_n 的位数是偶数时，取负号；当 a_n 的位数是奇数时，取正号.

于是，若数列中有一个数可以被 11 整除，则其后面的数也可以被 11 整除. 若 a_n 的位数是偶数，则

$\text{res}(a_n)=-\text{res}(b_n)$.

所以，$a_{n+1}=a_n+b_n$ 可以被 11 整除.

由条件可知 a_n 是严格递增的.

若 a_1 的位数是偶数，于是，当 $a_1\neq 10$ 时，a_2 是被 11 整除的合数；当 $a_1=10$ 时，$a_2=11$，$a_3=22$ 是被 11 整除的合数.

下面证明：当 a_7 的位数是奇数时，前六个数中有一个数的位数是偶数.

若 a_1、a_2、a_3、a_4、a_5、a_6 的位数都是奇数，设 c 是 a_1 的首位数字，d 是 a_1 的末位数字，则 $1\leqslant c\leqslant 9$，$0\leqslant d\leqslant 9$（如果 a_1 是一位数，则 $c=d$）.

所以，b_1 的首位数字为 d，末位数字为 c.

由于 $a_2=a_1+b_1$ 的位数是奇数位，所以，a_2 与 a_1 的位数相同，且有 $c+d<10$.

于是，a_2 的首位数字为 $c+d$ 或 $c+d+1$（这取决于第二位是否进位），末位数字为 $c+d$. 因此，a_2 的首位数字不小于 $c+d$.

同理，$a_3=a_2+b_2$ 的首位数字至少是 $2(c+d)$，$a_4=a_3+b_3$ 的首位数字至少是 $4(c+d)$，$a_5=a_4+b_4$ 的首位数字至少是 $8(c+d)$，$a_6=a_5+b_5$ 的首位数字至少是 $16(c+d)$.

因为 $1\leqslant c+d<10$，与 $16(c+d)<10$ 矛盾.

综上所述，a_7 总是合数.

证法 2 首先证明：若数 a_n 有偶数位，则 a_{n+1} 必为一个可以被 11 整除的合数.

记 $a_{2n}=10^{2n-1}b_{2n}+\cdots+10^1b_2+b_1$，则

$$a_{2n+1}=\sum_{i=1}^{n}(10^{2n-i}+10^{i-1})(b_i+b_{2n+1-i}).$$

而 $10^{2n-i}+10^{i-1}(i=1,2,\cdots,n)$ 都可以被 11 整除. 所以，a_{2n+1} 必为可以被 11 整除的数.

下面证明：奇数位数 a_n 至多经 6 次变换升位为偶数位.

若数 a_n 有 k 位，k 为奇数，则 a_{n+1} 至多有 $k+1$ 位. 这是因为

$$a_{n+1}\leqslant 2(10^{k+1}-1)=\underbrace{199\cdots98}_{k-1\text{个}}.$$

若 a_n 末位为 0，则 a_{n+1} 末位不能为 0，这是显然的.

若 a_n 变成 a_{n+1}，a_{n+1} 末位为 0，则它一定进行了升位，因为末位为 0 必为 $1+9$，$2+8$，$\cdots$.

所以，首位为 $1+9$，$2+8$，$\cdots$，从而进行了升位.

于是，若 a_n 变为 a_{n+1}，则 a_{n+1} 首项一定与末项相同，或首项比末项大 1（这是由不能进行升位为保证的).

我们考虑一种极端情况.

若首次项为 $\overline{1\times0}$，第二次位数不变，而第三次不可能是 $\overline{2\times1}$，至少为 $\overline{2\times2}$，于是，第四次可能为 $\overline{5\times4}$ 或 $\overline{4\times4}$，第五次即 a_5 若不进行升位则必为 $\overline{8\times8}$ 或 $\overline{9\times8}$. 所以，第六次必然升位为偶数位，得证.

c 是 a_1 的首位数字，d 是 a_1 的末位数字，则 $1\leqslant c\leqslant 9$，$0\leqslant d\leqslant 9$（如果 a_1 是一位数，则 $c=d$).

所以，b_1 的首位数字为 d，末位数字为 c.

例 30 （第 20 届爱尔兰数学奥林匹克题）求 2007! 的末尾连续的 0 的个数及其最末一位非零数字.

解 设 $F(k)=\left[\frac{2007}{k}\right](k\in\mathbf{N}_+)$，则素数 5 在 2007! 中出现的次数为

$$F(5)+F(5^2)+F(5^3)+\cdots.$$

因为 $5^5>2007$，上式即为

$F(5)+F(5^2)+F(5^3)+F(5^4)$.

经计算知

$F(5)=401$，$F(25)=80$，$F(125)=16$，$F(625)=3$.

故 5 在 2007！中出现的次数为 500.

又因为比 2007 小的正偶数有 1003 个，所以，2 在 2007！中至少出现 1003 次.

这说明，$10^{500}\mid 2007!$，但 $10^{501}\nmid 2007!$.

因此，2007！的末尾有 500 个连续的 0.

下面求最末一位非零数字.

首先注意以下两个事实：

对任意整数 k，有

$$(10k+1)(10k+3)(10k+7)(10k+9)\equiv -1\pmod{10}, \quad ①$$

及 $$\prod_{\substack{i=1\\ i\neq 5}}^{k}(10k+i)\equiv 6\pmod{10}. \quad ②$$

考虑从 1 到 1999 除去 5 的倍数的所有奇数的乘积，可将其分成 200 组如式①所示的乘积，故这些数模 10 后为 $(-1)^{200}=1$.

此外，$2001\times 2003\times 2007\equiv 1\pmod{10}$.

另一方面，如前所述，$F(5)=401$，即小于或等于 2007 的自然数中有 401 个 5 的倍数(其中，有 201 个是奇数). 因此，小于或等于 2007 的所有正奇数的乘积可表示为

$2007!!=M_1\times 5^{201}\times 401!!$，

其中，$M_1\equiv 1\pmod{10}$，$n!!$ 表示小于或等于 n 的所有正奇数的积.

类似地，$401!!=M_2\times 5^{40}\times 79!!$，

其中，$M_2\equiv(-1)^{40}\equiv 1\pmod{10}$；

$79!!=M_3\times 5^8\times 15!!$，

其中，$M_3\equiv(-1)^8\equiv 1\pmod{10}$；

$15!!=1\times 3\times 5\times 7\times 9\times 11\times 13\times 15=M_4\times 5^2$，

其中，$M_4\equiv 1\pmod{10}$.

因此，$2007!!=M\times 5^{251}$，

其中，$M=M_1M_2M_3M_4\equiv 1\pmod{10}$.

再考虑小于 2007 的所有正偶数的乘积，即 $1003!\times 2^{1003}$.

考虑 1000！中除去 5 的倍数的其他数的乘积，可将其分成 100 组如式②中所示的乘积，故这些数模 10 后为

$6^{100}\equiv 6\pmod{10}$.

此外 $1001\times1002\times1003\equiv6 \pmod{10}$.

因 1003 以下的自然数中有 200 个 5 的倍数，故

$1003!=N_1\times5^{200}\times200!$，

其中，$N_1\equiv6 \pmod{10}$.

类似地，

$200!=N_2\times5^{40}\times40!$，

其中，$N_2\equiv6^{20}\equiv6 \pmod{10}$；

$40!\equiv N_3\times5^8\times8!$，

其中，$N_3\equiv6^4\equiv6 \pmod{10}$；

$8!=N_4\times5$，

其中，$N_4\equiv2\times3\times4\times(-4)\times(-3)\times(-2)\equiv-6 \pmod{10}$.

因此，$1003!=N\times5^{249}$，

其中，$N\equiv N_1N_2N_3N_4\equiv-6 \pmod{10}$.

综上，有

$2007!=MN\times5^{500}\times2^{1003}=MN\times2^{503}\times10^{500}$，

其中，$MN\equiv-6\equiv4 \pmod{10}$.

又因为 $2^{503}\equiv8 \pmod{10}$，所以，

$MN\times2^{503}\equiv4\times8\equiv2 \pmod{10}$.

因此，2007! 最末一位非零数字为 2.

【模拟实战】

1. (1963 年基辅数学奥林匹克题) 已知数 $\overline{32※35717※}$ 能被 72 整除，求这两个星号所表示的数码.
2. (第 18 届爱尔兰数学奥林匹克题) 两个人 A 和 B 仅用数字 1，2，3，4，5 组成一个 2005 位数 N，每次只选择一个数码. 由 A 先选，然后 A，B 交替选数码. 当且仅当选取的数 N 能被 9 整除时，A 获胜. 问谁有获胜策略?
3. (第 17 届日本数学奥林匹克题) 求 $11^{12^{13}}$ 的十位数字 (其中，$11^{12^{13}}$ 表示 11 的 12^{13} 次幂).
4. (1971 年第 34 届莫斯科数学奥林匹克题) 给定数字 2^k，其中 k 是一个大于 3 的自然数. 证明不论怎样重排 2^k 的数码，都不能得到一个等于 2^n 的数，其中 n 为任意一个大于 k 的自然数.
5. (1981 年基辅数学奥林匹克题) 设 p 是大于 3 的素数，若 p^n (n 是自然数) 是 20 位数. 证明在这 20 个数码中至少有 3 个数码是相同的.

6. （第48届斯洛文尼亚数学奥林匹克题）是否存在满足以下条件的正整数 n：如果 n 是它的各位数字之和的倍数，那么，n 与其各位数字之和的乘积的各位数字之和等于3.
7. （第18届意大利数学奥林匹克题）在 4×4 的方格表中的每个小方格内填一个数1或2. 若任意一个 3×3 的方格表（共4个）中的9个数字之和能被4整除，而所有小方格内的16个数字之和不能被4整除，求这16个数字之和的最大值和最小值.
8. 用1，2，3，4，5，6这六个数码组成一个六位数 $\overline{abcdef}$，其中不同的字母代表1～6中不同的数码，要求前两个数码组成的两位数 $\overline{ab}$ 是2的倍数；并且还要求 $\overline{abc}$ 是3的倍数；$\overline{abcd}$ 是4的倍数；$\overline{abcde}$ 是5的倍数；$\overline{abcdef}$ 是6的倍数，试找出所有这样的六位数，并说明你的推理过程.
9. 求 $(\sqrt{2}+\sqrt{5})^{2000}$ 的十进制表示中小数点前第一位数字和小数点后第一位数字.
10. （1991年第6届拉丁美洲数学竞赛题）N 是由5个不同的非零数码组成的5位数，且 N 等于这5个数码中取3个不同的数码构成的所有三位数的和，求所有的这种5位数 N.
11. （第54届白俄罗斯数学奥林匹克题）在十进制表示中，若 k 位数码 a 满足：如果两个均以 a 结尾的正整数的乘积也以 a 结尾，我们就称 a 是"稳定"的（如0和25稳定）. 证明：对任意正整数 k，恰存在四个稳定的 k 位数码.
12. 若干个整数的和能被6整除，证明这些数的立方和也能被6整除.
13. 设 n 是正整数. 证明：$n(n^2-1)(n^2-5n+26)$ 被120整除.
14. （1990年第7届巴尔干数学竞赛题）设 $a_1=1$，$a_2=3$，且对所有的正整数 n，
$$a_{n+2}=(n+3)a_{n+1}-(n+2)a_n.$$
求所有使 a_n 可被11整除的 n 的值.
15. 证明对于同样的整数 x 和 y，$2x+3y$ 和 $9x+5y$ 能同时被17整除.
16. （1988年第6届美国数学邀请赛题）试找出最小的正整数 n，使它的立方的末三位数字是888.
17. （2002—2003年度英国数学奥林匹克题）已知 $34!=295\ 232\ 799\ cd9\ 604\ 140\ 847\ 618\ 609\ 643\ 5ab\ 000\ 000$.
求数字 a，b，c，d 的值.

第八章　平方数

【基础知识】

1．若 a 是整数，则 a^2 叫做 a 的平方数（许多人习惯称完全平方数）.

2．平方数的因数具有如下特征：

（1）n^2 的标准分解式中，每个素因数的指数都是偶数.

（2）若 $n^2=a^2b$（a，b 是整数）为平方数，则 b 为平方数.

（3）若 $n^2=ab$（a，b 是互素的整数）为平方数，则 a，b 都为平方数.

3．在平方数 n^2 的十进制表达式中，其数字具有如下一些特征：

（1）n^2 的个位数字为 0，1，4，5，6，9.

（2）n^2 的十位数字为奇数，当且仅当 n^2 的个位数字为 6.

（3）n^2 的个位数字为 5，则 n^2 的十位数字为 2，百位数是偶数.

上述特征可概括为：平方数的末两位只能是$\overline{\text{偶}0}$、$\overline{\text{偶}1}$、$\overline{\text{偶}4}$、$\overline{\text{偶}9}$、$\overline{25}$、$\overline{\text{奇}6}$之一.

（4）奇数的平方的十位数是偶数.

（5）把平方数的各位数码相加，如果所得到的和不是一位数，再把这个和的各位数码相加，直到一位数为止，这个一位数只能是 0，1，4，7，9.

4．在平方数 n^2 的十进制表达式中，其有关模下的余数或被 4，8，3，5 除时的余数具有如下一些特征：

（1）$n^2\equiv 0，1 \pmod{3，4}$.

（2）$n^2\equiv 0，1，4 \pmod{5，8}$.

（3）$n^2\equiv 0，1，4，7 \pmod 9$.

（4）$n^2\equiv 0，1，4，5，6，9 \pmod{10}$.

（5）偶数的平方能被 4 整除，奇数的平方被 4 除余 1.

（6）偶数的平方被 8 除余 0 或 4，奇数的平方被 8 除余 1.

（7）若一个整数能被 3 整除，则这个数的平方能被 3 整除；若一个整数不能被 3 整除，则这个数的平方被 3 除余 1.

（8）若一个整数能被 5 整除，则这个数的平方能被 5 整除；若一个整数不能被 5

整除，则这个数的平方被 5 除余+1 或−1.

5. 平方数序列的间距具有如下特征：

(1) $m^2-n^2\geqslant 3$ $(0<n<m,\ m,\ n\in\mathbf{N})$；

(2) m^2 与$(m+1)^2$ 之间不存在平方数，即：若 $m^2<p<(m+1)^2$，则 p 不是平方数.

6. 平方数的约数有如下特征：

(1) 平方数的所有正约数个数为奇数，并且反过来也成立.

(2) 如果素数 p 是一个平方数的约数，那么 p^2 也是这个平方数的约数.

【典型例题与基本方法】

例 1 （第 24 届希腊数学奥林匹克题）求所有自然数 n，使得 $2007+4^n$ 为平方数.

解 设 $2007+4^n=k^2$ $(k\in\mathbf{N})$，则

$$k^2-4^n=2007$$

$$\Leftrightarrow k^2-2^{2n}=2007$$

$$\Leftrightarrow (k-2^n)(k+2^n)=1\times3\times3\times223.$$

又 $k-2^n<k+2^n$，由上面的等式得

$$\begin{cases}k-2^n=1,\\k+2^n=2007\end{cases}\quad ①$$

或 $$\begin{cases}k-2^n=3,\\k+2^n=669\end{cases}\quad ②$$

或 $$\begin{cases}k-2^n=9,\\k+2^n=223.\end{cases}\quad ③$$

由方程组①得 $2^n=1003$，矛盾；

由方程组②得 $2^n=333$，矛盾；

由方程组③得 $2^n=107$，矛盾.

因此，不存在自然数 n，使得 $2007+4^n$ 为平方数.

例 2 （1975 年基辅数学奥林匹克题）证明不存在这样的三位数$\overline{abc}$，使$\overline{abc}+\overline{bca}+\overline{cab}$为平方数.

证明 设 $n=\overline{abc}+\overline{bca}+\overline{cab}$，则

$$\begin{aligned}n&=(100a+10b+c)+(100b+10c+a)+(100c+10a+b)\\&=111(a+b+c)\\&=3\cdot37(a+b+c).\end{aligned}$$

若 n 为完全平方数，则可设 $n=m^2$.

$m^2=3\cdot 37(a+b+c)$.

于是 m 是 37 的倍数，从而可设 $m=37k$，则

$$37k=3(a+b+c). \quad ①$$

由于 $1\leqslant a+b+c\leqslant 27$ 以及 3 与 37 互素，则①式不可能成立.

于是 n 不是完全平方数.

例 3 （2002 年澳大利亚数学奥林匹克题）设 m 和 n 是正整数，且满足

$$2001m^2+m=2002n^2+n.$$

证明：$m-n$ 是完全平方数.

证明 由已知条件知 $m>n$. 设 $m=n+k$，其中 k 为正整数，则原方程化为

$$n^2-4002nk-2001k^2-k=0.$$

将上式看成关于 n 的二次方程，且根 n 为整数，则判别式是完全平方数，即存在整数 D，使得

$$D^2=(4002k)^2+4(2001k^2+k)，即$$

$$\left(\frac{D}{2}\right)^2=k[(2001^2+2001)k+1].$$

因为 $(k,(2001^2+2001)k+1)=1$，则 k 和 $(2001^2+2001)k+1$ 均为完全平方数.

所以，$m-n=k$ 是完全平方数.

例 4 证明：存在无限正整数序列 $\{a_n\}$，使得 $\sum\limits_{k=1}^{n}a_k^2$ 对于任意正整数 n 是一个完全平方数.

证明 记 $S_n=\sum\limits_{k=1}^{n}a_k^2$.

从勾股数组 (a, b, c) 开始，取 a 为奇数，b 为偶数 [例如 $(3, 4, 5)$]，奇数 a 为 a_1，偶数 b 为 a_2. 这一定意味着 $S_1=a^2$ 和 $S_2=a^2+b^2=c^2$ 是完全平方. 可选取其他的 a_n 为偶数，使得

$$S_{n+1}=S_n+a_{n+1}^2=(a_{n+1}+1)^2$$

成立. 这是可能的，由于

$$S_{n+1}-a_{n+1}^2=S_n$$

$$\Leftrightarrow(a_{n+1}+1)^2-a_{n+1}^2=(a_n+1)^2$$

$$\Leftrightarrow 2a_{n+1}+1=(a_n+1)^2$$

$$\Leftrightarrow a_{n+1}=\frac{(a_n+1)^2-1}{2}$$

$$\Leftrightarrow a_{n+1}=\frac{a_n(a_n+2)}{2}.$$

因为 a_n 为偶数的选择表示 a_n+2 一定也是偶数，故 $\frac{a_n(a_n+2)}{2}$ 也是偶数.

例如，取 $a_1=3$，$a_2=4$，得数列 3，4，12，84，3612，…，满足题目要求.

例 5 （1990 年前苏联教委推荐试题）试问能否找到四个自然数，使得其中每两个数的乘积与 1990 的和都是完全平方数.

解 由于奇数的平方被 4 除余 1，偶数的平方被 4 除余 0，而 1990 被 4 除余 2.

于是若两数之积与 1990 之和为完全平方数，则这两数之积被 4 除只能余 2 或余 3.

因此，若存在这样的四个自然数，则至多有一个是偶数. 否则若有两个偶数，则其积与 1990 之和被 4 除余 2 不可能是平方数.

因而，这四个自然数中至少有三个奇数. 由于奇数被 4 除余 1 或余 3，则必定有两个奇数对模 4 同余. 然而

$(4k_1+1)(4k_2+1)=4(4k_1k_2+k_1+k_2)+1$,

$(4k_1+3)(4k_2+3)=4(4k_1k_2+3k_1+3k_2+2)+1$.

于是，这两个奇数之积与 1990 之和被 4 除余 3，因而不可能是完全平方数.

由以上，不存在符合题目要求的四个自然数.

例 6 （1996 年上海市高中数学竞赛题）设 $k_1<k_2<k_3<\cdots$ 是正整数，且没有两个是相邻的，又对于 $m=1, 2, 3, \cdots$，$S_m=k_1+k_2+\cdots+k_m$. 求证：对每一个正整数 n，区间 $[S_n, S_{n+1})$ 中至少含有一个完全平方数.

证明 区间 $[S_n, S_{n+1})$ 中至少含有一个完全平方数的充要条件是 $[\sqrt{S_n}, \sqrt{S_{n+1}})$ 中至少含有一个整数.

因此，要证本题，只需证明对每个 $n\in\mathbf{N}$，都有

$\sqrt{S_{n+1}}-\sqrt{S_n}\geqslant 1$.

这等价于 $\sqrt{S_{n+1}}\geqslant\sqrt{S_n}+1$，即

$S_n+k_{n+1}\geqslant(\sqrt{S_n}+1)^2$，即

$k_{n+1}\geqslant 2\sqrt{S_n}+1$.

因为 $k_{m+1}-k_m\geqslant 2$，所以

$$S_n=k_n+k_{n-1}+\cdots+k_1$$

$$\leqslant\begin{cases} k_n+(k_n-2)+\cdots+2=\dfrac{k_n(k_n+2)}{4}, & k_n \text{ 是偶数时;} \\ k_n+(k_n-2)+\cdots+1=\dfrac{(k_n+1)^2}{4}, & k_n \text{ 是奇数时} \end{cases}$$

$$\leqslant\frac{(k_n+1)^2}{4},$$

于是得 $k_n+1\geqslant 2\sqrt{S_n}$，从而

$$k_{n+1}\geqslant k_n+2\geqslant 2\sqrt{S_n}+1.$$

这就是我们所要证明的. 故原命题得证.

例 7 （2002 年澳大利亚国家数学竞赛题）求所有素数 p，q，r，使得 p^q+p^r 为完全平方数.

解 若 $q=r$，则 $p^q+p^r=2p^q$，所以，$p=2$，q 为奇素数. 故 $(2, q, q)$ 为满足条件的三元素数组，其中素数 $q\geqslant 3$.

若 $q\neq r$，不失一般性，设 $q<r$，则

$p^q+p^r=p^q(1+p^s)$，其中 $s=r-q\geqslant 1$.

由于 p^q 和 $1+p^s$ 的最大公因数为 1，所以，p^q 和 $1+p^s$ 均为完全平方数，故 $q=2$.

由于 $1+p^s$ 为完全平方数，设 $1+p^s=u^2$，即

$p^s=u^2-1=(u+1)(u-1)$.

因为 $u+1$ 与 $u-1$ 的最大公因数为 1 或 2，故当最大公因数为 2 时，u 为奇数，p 为偶数，即 $p=2$，且 $u-1$ 和 $u+1$ 均为 2 的幂. 于是 $u=3$. 从而 $1+2^s=3^2$，所以，

$s=3$，$r=q+s=2+3=5$.

故满足条件的三元素数组为

$(2, 2, 5)$ 和 $(2, 5, 2)$.

当 $u+1$ 和 $u-1$ 的最大公因数为 1 时，u 为偶数，$u-1$ 必须为 1，否则 $u-1$ 和 $u+1$ 可表示为不同奇素数的乘积，所以，不可能是一个素数的整数次幂. 于是，

$u=2, p^s=(u-1)(u+1)=3, p=3, s=1,$

$r=q+s=3.$

故满足条件的三元素数组为

$(3,2,3)$ 和 $(3,3,2)$.

综上所述，原命题的解为

$(2,2,5)$，$(2,5,2)$，$(3,2,3)$，$(3,3,2)$，$(2,q,q)$，其中素数 $q\geqslant 3$.

例 8 （1980 年列宁格勒数学奥林匹克题）求出所有的素数 p，使得 $2p^4-p^2+16$ 是一个完全平方数.

解法 1 当 $p=2$ 时，$2p^4-p^2+16=44$ 不是完全平方数.

所以 p 是奇素数.

设 $2p^4-p^2+16=k^2$，其中 k 是奇数，则

$p^2(2p^2-1)=(k-4)(k+4)$.

因为 p 是素数,因此 $p|k-4$ 或 $p|k+4$,但 p 不能同时整除 $k-4$ 和 $k+4$,否则

$p|(k+4)-(k-4)=8$,

这与 p 为奇素数矛盾.

因此 $k+4$ 与 $k-4$ 中有且只有一个能被 p^2 整除.

若 $p^2|k-4$,设 $k-4=sp^2$,这里 s 是奇数,于是

$k+4=sp^2+8$,从而

$p^2(2p^2-1)=(k+4)(k-4)=sp^2(sp^2+8)$,即

$s(sp^2+8)=2p^2-1$,即

$(s^2-2)p^2=-8s-1$.

此式的右边为负数,所以只能有 $s=1$.

这时　$p^2=9$,$p=3$.

而当 $p=3$ 时,$2p^4-p^2+16=169$ 是完全平方数.

如果 $p^2|k+4$,设 $k+4=sp^2$,则 s 是奇数,于是

$k-4=sp^2-8$,

$(s^2-2)p^2=8s-1$.

当 $s=1$ 时,有 $-p^2=7$,这不可能.

当 $s\geqslant 3$ 时,由于

$$\begin{aligned}(s^2-2)p^2&>(s^2-4)p^2=(s+2)(s-2)p^2\geqslant 5\cdot 9(s-2)\\&=(8s-1)+(37s-89)\geqslant(8s-1)+(111-89)>8s-1.\end{aligned}$$

这也出现矛盾.

综合以上,当且仅当 $p=3$ 时,$2p^4-p^2+16$ 才是平方数.

解法 2　当 $p=2$ 时,$2p^4-p^2+16=44$ 不是完全平方数.

当 $p\geqslant 3$ 时,若 $3\nmid p$,则

$p^2\equiv 1 \pmod 3$,

$2p^4-p^2+16\equiv 2 \pmod 3$,

此时 $2p^4-p^2+16$ 不是平方数.

于是 $3|p$,又 p 是素数,所以 $p=3$.

而当 $p=3$ 时,$2p^4-p^2+16=169$ 是平方数.

例 9　(CMO-7 试题)已知整数列$\{a_0,a_1,a_2,\cdots\}$满足

(1) $a_{n+1}=3a_n-3a_{n-1}+a_{n-2}$,$n=2,3,\cdots$;

(2) $2a_1=a_0+a_2-2$;

(3) 对任意自然数 m,在数列$\{a_0,a_1,a_2,\cdots\}$中必有相继的 m 项 a_k,a_{k+1},$\cdots$,a_{k+m-1}都是完全平方数.

求证$\{a_0, a_1, a_2, \cdots\}$的所有项都是完全平方数.

证法 1　由条件（1）知

$a_{n+1}-a_n=2(a_n-a_{n-1})-(a_{n-1}-a_{n-2})$.

记$d_n=a_n-a_{n-1}$，$n=1, 2, \cdots$，则

$d_{n+1}-d_n=d_n-d_{n-1}=\cdots=d_2-d_1$.

由条件（2）得

$d_2-d_1=a_2-2a_1+a_0=2$,

所以有

$$a_n=a_0+\sum_{k=1}^{n}d_k=a_0+nd_1+n(n-1),$$

即　$a_n=n^2+bn+c$，$n=0, 1, 2, \cdots$,

其中$b=a_1-a_0-1$，$c=a_0$.

由条件（3）知，存在非负整数t，使得a_t和a_{t+2}都是完全平方数，从而

$a_{t+2}-a_t\not\equiv 2 \pmod 4$.

又$a_{t+2}-a_t=(t+2)^2+b(t+2)-t^2-bt=4t+4+2b$,

所以b是偶数. 令$b=2\lambda$，则

$$\begin{aligned}a_n&=n^2+2\lambda n+c\\&=(n+\lambda)^2+c-\lambda^2.\end{aligned}\qquad①$$

下面证明$c-\lambda^2=0$.

否则，若$c-\lambda^2\neq 0$，则$c-\lambda^2$的不同约数只有有限多个，设其个数为m.

由a_n的通项公式可知，存在n_0使得当$n\geqslant n_0$时，数列$\{a_n\}$严格单调递增.

由条件（3），存在$k\geqslant n_0$，使得

$a_{k+i}=p_i^2$，$i=0, 1, 2, \cdots, m$.

其中p_i为非负整数，且$p_0<p_1<p_2<\cdots<p_m$.

由此可知

$c-\lambda^2=a_n-(n+\lambda)^2=p_i^2-(k+i+\lambda)^2=(p_i-k-i-\lambda)(p_i+k+i+\lambda)$,

其中，$i=0,1,2,\cdots,m$.

这与$c-\lambda^2$只有m个不同约数矛盾.

于是$c-\lambda^2=0$.

由①式，$a_n=(n+\lambda)^2$，$n=0,1,2,\cdots$.

即数列$\{a_0, a_1, a_2, \cdots\}$的所有项都是完全平方数.

证法 2　由证法 1 得

$a_n=n^2+bn+c$.

从而存在 n_0，使得当 $n\geqslant n_0$ 时，数列$\{a_n\}$严格单调递增，且

$$0<\left(n-\frac{|b|+1}{2}\right)^2\leqslant a_n\leqslant\left(n+\frac{|b|+1}{2}\right)^2.$$

于是有

$$0<\sqrt{a_{n+1}}-\sqrt{a_n}=\frac{a_{n+1}-a_n}{\sqrt{a_{n+1}}+\sqrt{a_n}}<\frac{2n+1+b}{2\sqrt{a_n}}\leqslant\frac{2n+1+b}{2n-|b|-1}.$$

由此可知，存在 $n_1\geqslant n_0$，使得当 $n\geqslant n_1$ 时，

$$0<\sqrt{a_{n+1}}-\sqrt{a_n}<2. \qquad ②$$

利用条件 (3)，易知存在 $k\geqslant n_1$，使得 a_k 和 a_{k+1} 都是完全平方数，所以由②有

$$\sqrt{a_{k+1}}-\sqrt{a_k}=1.$$

记 $\sqrt{a_k}=t$.

由 $a_n=n^2+bn+c$ 可得

$$a_{n+1}=2a_n-a_{n-1}+2,\ n=1,\ 2,\ \cdots.$$

所以由 $\sqrt{a_k}=t$，即 $a_k=t^2$ 得

$$a_{k+2}=2(t+1)^2-t^2+2=(t+2)^2,$$

$$a_{k-1}=2t^2-(t+1)^2+2=(t-1)^2.$$

于是，用数学归纳法易证，数列$\{a_0, a_1, a_2, \cdots\}$的所有项都是完全平方数.

例 10 （IMO-44 预选题）一个整数 n 若满足$|n|$不是一个完全平方数，则称这个数是“好”数. 求满足下列性质的所有整数 m：整数 m 可以用无穷多种方法表示成三个不同的“好”数的和，且这三个“好”数的积是一个奇数的平方.

解 假设 m 可以表示为 $m=u+v+w$，且 uvw 是一个奇数的平方. 于是，u，v，w 均为奇数，且 $uvw\equiv1 \pmod 4$. 所以，u，v，w 中要么有两个数模 4 余 3，要么没有一个数模 4 余 3. 无论哪种情况，均有

$$m=u+v+w\equiv3 \pmod 4.$$

下面证明，当 $m=4k+3$ 时，满足条件要求的性质. 为此，我们寻求形如

$$4k+3=xy+yz+zx$$

的表达式. 在这样的表达式中，三个被加数的积是一个完全平方数.

设 $x=2l+1$，$y=1-2l$，从而，可推出

$$z=2l^2+2k+1.$$

于是，有

$$xy=1-4l^2=f(l),$$

$$yz=-4l^3+2l^2-(4k+2)l+2k+1=g(l),$$

$$zx=4l^3+2l^2+(4k+2)l+2k+1=h(l).$$

由上面的表达式可知，$f(l)$，$g(l)$，$h(l)$均为奇数，且乘积是一个奇数的平方．同时易知，除了有限个 l 外，$f(l)$，$g(l)$，$h(l)$是互不相同的．

下面证明对于无穷多个 l，使$|f(l)|$，$|g(l)|$，$|h(l)|$不是完全平方数．

当 $l\neq0$ 时，$|f(l)|$不是完全平方数．

选取两个不同的素数 p，q，使得

$p>4k+3$，$q>4k+3$．

选取 l，使得 l 满足

$1+2l\equiv0 \pmod p$，$1+2l\not\equiv0 \pmod{p^2}$，

$1-2l\equiv0 \pmod q$，$1-2l\not\equiv0 \pmod{q^2}$，

由孙子定理（即中国剩余定理）知如上的 l 是存在的．

由于 $p>4k+3$，且

$$\begin{aligned}2(2l^2+2k+1)&=(2l+1)(2l-1)+4k+3\\&\equiv4k+3 \pmod p,\end{aligned}$$

所以，$2(2l^2+2k+1)$不能被 p 整除．

从而，$2l^2+2k+1$ 也不能被 p 整除．

于是，$|h(l)|=|(2l+1)(2l^2+2k+1)|$能被 p 整除，但不能被 p^2 整除．

因此，$|h(l)|$不是完全平方数．

类似地可得$|g(l)|$也不是完全平方数．

【解题思维策略分析】

1．关注平方数的因数特征

例 11 （2002 年西部数学奥林匹克题）求所有的正整数 n，使得

$n^4-4n^3+22n^2-36n+18$

是一个完全平方数．

解 我们记

$A=n^4-4n^3+22n^2-36n+18=(n^2-2n)^2+18(n^2-2n)+18$．

令 $n^2-2n=x$，$A=y^2$，y 为非负整数，则

$(x+9)^2-63=y^2$，即$(x+9-y)(x+9+y)=63$．

可知只能是$(x+9-y,x+9+y)=(1,63)$，$(3,21)$或$(7,9)$．分别得$(x,y)=(23,31)$，$(3,9)$或$(-1,1)$．其中只有 $x=3$ 和-1时，$n^2-2n=x$ 有正整数解，得 $n=1$ 或 3．

所以，满足条件的 $n=1$ 或 3．

注：此题亦可利用不等式处理．

例 12 （2005 年英国数学奥林匹克题）已知 N 为正整数，恰有 2005 个正整数

有序对 (x, y) 满足$\frac{1}{x}+\frac{1}{y}=\frac{1}{N}$. 证明：$N$ 是完全平方数.

证明 首先，注意到 x，$y>N$，否则$\frac{1}{x}$或$\frac{1}{y}$之一将大于$\frac{1}{N}$，则

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{N}$$
$$\Rightarrow\frac{x+y}{xy}=\frac{1}{N}$$
$$\Rightarrow N(x+y)=xy$$
$$\Rightarrow(x-N)(y-N)=N^2$$
$$\Rightarrow y=\frac{N^2}{x-N}+N.$$

这样，(x,y)是一组解当且仅当$(x-N)\mid N^2$.

另外，N^2 的每个正因子 d 都对应着一组唯一解$\left(x=d+N, y=\frac{N^2}{d}+N\right)$. 因此，在有序解$(x,y)$和 N^2 的正因子间存在一个双射.

令 $N=p_1^{q_1}p_2^{q_2}\cdots p_n^{q_n}$，则

$N^2=p_1^{2q_1}p_2^{2q_2}\cdots p_n^{2q_n}$.

而 N^2 的任一正因子必有形式 $p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$，其中 $0\leqslant a_i\leqslant 2q_i$，$i=1$，2，…，$n$. 每个因子中 p_i 的指数有 $2q_i+1$ 种可能，所以，得到 N^2 的

$(2q_1+1)(2q_2+1)\cdots(2q_n+1)$

个正因子. 这样，

$(2q_1+1)(2q_2+2)\cdots(2q_n+1)=2005=5\times401$.

而 401 是素数，故 2005 的正因子仅为 1，5，401，2005. 因为所有这些因子都模 4 余 1，对所有 q_i 有 $2q_i+1\equiv1 \pmod 4$，所以，$q_i\equiv0 \pmod 2$. 既然所有素因子的指数都为偶数，故 N 是完全平方数.

例 13 （1986 年第 49 届莫斯科数学奥林匹克题）已知 48 个自然数的乘积中恰好有 10 个不同的素因数. 证明由这 48 个自然数中可以挑出 4 个数来，它们的乘积是一个完全平方数.

证明 将这 48 个自然数进行素因数分解，并将这 48 个自然数中任何两数 a，b 之积都表示成最大可能的平方数和一些素数的一次幂的乘积的形式［例如 $a=2^{13}\cdot3^4\cdot19^3$，$b=5^6\cdot7^7\cdot19$，则 $ab=(2^6\cdot3^2\cdot5^3\cdot19^2)^2\cdot2\cdot7$］，再用 ab 除以最大可能的平方数，得到的商就是一些素数一次幂的乘积，以这些素数为元素得到一个素数集合（如上述的 ab 得到素数集合$\{2,7\}$）.

这样我们就得到每一数对 (a, b) 与素数集合的一个对应.

由于这 48 个数两两组成的数对 (a, b) 共可能有 $C_{48}^2=\frac{48\cdot 47}{2}=1128$ 对，而这 48 个自然数之乘积恰有 10 个不同的素因数，这 10 个素因数组成的集合共有 $2^{10}=1024$ 个子集.

由于 $1128>1024$，所以必可找到两个不同的数对 (a,b) 和 (c,d)，它们对应着同一个素数集 $(p_1,p_2,\cdots,p_k)(0\leqslant k\leqslant 10)$，即

$ab=m^2p_1p_2\cdots p_k$,

$cd=n^2p_1p_2\cdots p_k$.

于是 $abcd=(mnp_1p_2\cdots p_k)^2$ 是一个完全平方数.

如果两个数对 (a,b) 和 (c,d) 没有公共元素，则 a，b，c，d 即为所求.

如果两个数对 (a,b) 和 (c,d) 有公共元素，不妨设 $b=d$，则 ac 一定是完全平方数.

从这 48 个自然数中，暂时去掉 a 和 c，还有 46 个元素，对这 46 个自然数做同样的考虑.

由于 46 个数的乘积仍仅有不超过 10 个的不同的素因数，并且 $C_{46}^2=\frac{46\cdot 45}{2}=1035>1024=2^{10}$，所以一定可以从中找出两个不同的数对 (x,y) 和 (z,t)，使得 $xyzt$ 是完全平方数.

如果数对 (x,y) 和 (z,t) 没有公共元素，则 x，y，z，t 即为所求.

如果数对 (x,y) 和 (z,t) 有公共元素，设为 $x=t$，那么 yz 必为完全平方数，此时 $acyz$ 也为完全平方数，a，c，y，z 即为所求.

例 14 （2005 年克罗地亚数学竞赛题）已知正整数 a，b，c 满足 $c(ac+1)^2=(5c+2b)(2c+b)$.

(1) 若 c 为奇数，证明：其为完全平方数.

(2) 问：c 是否能为偶数？

解 记 x 和 y 的最大公因子为 $M(x,y)$.

(1) 设 $d=M(b,c)$，$b=db_0$，$c=dc_0$，则

$M(b_0,c_0)=1$.

于是，所给等式化为

$c_0(cdc_0+1)^2=d(5c_0+2b_0)(2c_0+b_0)$.

因为 b_0 和 c_0 互素，所以，

$M(c_0,2c_0+b_0)=1$.

又因为 c_0 为与 b_0 互素的奇数，所以，

$M(c_0,5c_0+2b_0)=M(c_0,2b_0)=1$.

于是，$c_0|d$.

由于 $M(d,(abc_0+1)^2)=1$，所以，$d|c_0$.

因此，$c_0=d$. 故 $c=dc_0=d^2$.

(2) 假设 c 为偶数，即 $c=2c_1$.

由所给等式得

$c_1(2ac_1+1)^2=(5c_1+b)(4c_1+b)$.

设 $d=M(b,c_1)$，$b=db_0$，$c_1=dc_0$，则

$M(b_0,c_0)=1$.

于是，上式化为

$$c_0(2abc_0+1)^2=d(5c_0+b_0)(4c_0+b_0). \quad ①$$

因为 $M(c_0,5c_0+b_0)=M(c_0,4c_0+b_0)=1$,

$M(d,(2adc_0+1)^2)=1$,

则 $d=c_0$，$(2abc_0+1)^2=(5c_0+b_0)(4c_0+b_0)$.

注意到

$M(5c_0+b_0,4c_0+b_0)=M(c_0,4c_0+b_0)=M(c_0,b_0)=1$,

则式①右边的两个因式均为完全平方.

设 $5c_0+b_0=m^2$，$4c_0+b_0=n^2$，其中 m，$n\in\mathbf{Z}$，于是，$m>n$，即

$m-n\geqslant1$，$d=c_0=m^2-n^2$,

$2ad^2+1=2adc_0+1=mn$.

$$\begin{aligned}\text{则 } mn&=1+2ad^2=1+2a(m^2-n^2)^2\\&=1+2a(m-n)^2(m+n)^2\\&\geqslant1+2a(m+n)^2\\&\geqslant1+8amn\\&\geqslant1+8mn.\end{aligned}$$

所以，$7mn\leqslant-1$，矛盾.

因此，c 不能为偶数.

例 15 （2006 年英国数学奥林匹克题）设 n 是整数. 若 $2+2\sqrt{1+12n^2}$ 是整数，求证：该数是完全平方数.

证明 由 $2+2\sqrt{1+12n^2}\in\mathbf{Z}$ ($n\in\mathbf{Z}$)，得 $1+12n^2$ 是完全平方数.

设 $1+12n^2=m^2$ ($m\in\mathbf{N}_+$)，则

$(m+1)(m-1)=12n^2$.

又 $m+1$，$m-1$ 奇偶性相同，故 $m+1$，$m-1$ 均为偶数.

则$\frac{m+1}{2}\cdot\frac{m-1}{2}=3n^2$.

记$\frac{m+1}{2}=t$，则$\frac{m-1}{2}=t-1$ ($t\in\mathbf{N}_+$).

故 $t(t-1)=3n^2$. ①

要证 $2+2\sqrt{1+12n^2}=2+2m$ 是完全平方数，只须证 t 是完全平方数.

由式①知，$3|t$ 或 $3|(t-1)$，而 $\gcd(t,t-1)=1$.

若 $3|t$，则由 $\gcd\left(\frac{t}{3},t-1\right)=1$，且$\frac{t}{3}(t-1)=n^2$，知 $\frac{t}{3}$ 与 $t-1$ 都是完全平方数.

设$\frac{t}{3}=k^2$，则 $t=3k^2$，知 $t-1=3k^2-1\equiv-1 \pmod 3$不可能是完全平方数. 矛盾.

因此，$3|(t-1)$.

从而，由 $\gcd\left(t,\frac{t-1}{3}\right)=1$，$t\cdot\frac{t-1}{3}=n^2$，知 t 与$\frac{t-1}{3}$都是完全平方数.

综上所述，原结论成立.

例 16 （1973 年基辅数学奥林匹克题）将 2^n 个素数写成一行. 已知其中不同的数少于 n 个，证明，可以从上述数列中选取一组写在一起的数，它们的乘积是一个完全平方数.

证明 要证明本题的结论，只要证明在某一组连续排列的数中，每一个素数都出现偶数次即可.

设所给的 2^n 个素数为 a_1，a_2，…，a_{2^n}，其中不同的素数有 m 个：

p_1，p_2，…，p_m，$m<n$.

设所给素数第 1 项至第 j 项的乘积 $a_1a_2\cdots a_j$ ($1\leqslant j\leqslant 2^n$) 中素数 p_i ($1\leqslant i\leqslant m$) 的指数记为 c_{ij}.

又设 d_{ij} 为 c_{ij} 被 2 除所得的余数：

$c_{ij}=2l_{ij}+d_{ij}$，$d_{ij}\in\{0,1\}$.

形如$(d_{1j},d_{2j},d_{3j},\cdots,d_{mj})$的每一个数组都是由 m 个 0 或 1 组成.

由于 $j=1$，2，…，2^n，所以这样的数组共有 2^n 个. 而由 m 个 0 或 1 组成的数组总共只有 2^m 个.

由于 $m<n$，则 $2^m<2^n$，所以在构造的 2^n 个数组中一定有两个相同的数组，设为

$$(d_{1j},d_{2j},\cdots,d_{mj})=(d_{1k},d_{2k},\cdots,d_{mk}),$$

其中 $1\leqslant j<k\leqslant 2^n$.

这时相应的 c_{ij}，c_{ik}就有

$c_{ik}-c_{ij}=2(l_{ik}-l_{ij})+(d_{ik}-d_{ij})=2(l_{ik}-l_{ij})$.

于是 $c_{ik}-c_{ij}$ 为偶数.

考虑到 c_{ij} 的定义，则在乘积

$$a_{j+1}a_{j+2}\cdots a_k=\frac{a_1a_2\cdots a_k}{a_1a_2\cdots a_j}$$

中，素数 p_i 的指数等于 $c_{ik}-c_{ij}$ 次，即 p_i 的指数为偶数次. 于是 $a_{j+1}a_{j+2}\cdots a_k$ 为完全平方数.

2. 关注平方数的数字特征

例 17 求出所有不超过 10^3 的这样正整数，它的平方的末两位数字相同，但不是零.

解 非零整数平方末尾数只能是 1，4，5，6，9.

整数的平方末两位数不能为相同的奇数：11，55，99. 否则对于奇数 n，$4\mid n^2-1$，但 10，54，98 不能被 4 整除.

偶数 n 的平方末两位数不可能是 66，否则 $4\mid n^2$，但 $4\nmid 10^2l+66$.

从而仅剩下末两位是 44，我们只要在 1 到 50 中找出这样的数就行了，这是因为 m 和 $50k+m$ 的平方有相同末两位数.

因为仅当整数的末尾数是 2 或 8 时，平方的末尾数才是 4. 容易找到在 1 到 50 中只有 12 和 38 两个数的平方末两位是 44. 因此，形如 $50k+12$ 和 $50k+38$ 的数具有我们所需要的性质.

在 1000 以内，这样的数有 40 个，只要取 $k=0$，1，2，…，19，就得到全部要求的数：12，38，62，88，…，962，988.

例 18 若 $24a^2+1=b^2$，求证：a，b 中有且仅有一个为 5 的倍数.

证明 只要证明 a，b 中不可能都是 5 的倍数，也不可能都不是 5 的倍数.

a，b 都不是 5 的倍数是显然的，下面证明不可能都不是 5 的倍数.

若 a^2，b^2 同为 $5k-1$ 型的数，则 b^2-a^2 可被 5 整除，而 $b^2-a^2=23a^2+1$.

考察 $23a^2+1$ 的末尾数. 由于 a^2 尾数只能是 0，1，4，5，6，9，所以 $23a^2+1$ 末尾数只能是 1，4，3，6，9，8. 因此 $23a^2+1$ 不能被 5 整除，即 a^2，b^2 不能同为 $5k+1$ 或 $5k-1$ 型的数.

若 a^2，b^2 中一个为 $5k+1$ 型的数，另一个为 $5k-1$ 型的数，则 a^2+b^2 可被 5 整除，而 $a^2+b^2=25a^2+1$，且 $25a^2+1$ 不能被 5 整除. 即这种情况也不可能.

因此，a，b 中有且仅有一个能被 5 整除.

例 9 （1962 年基辅数学奥林匹克题）求所有不超过 1000 的这样的整数，它的平方的末两位数码相同，但不等于零.

解 注意到平方数的个位不等于零，因此平方数的个位数只能是

1，4，5，6，9.

首先，完全平方数的末两位数码不可能都是奇数.

这是因为奇数的平方的十位数是偶数，而个位数是奇数.

因此，完全平方数的末两位不可能是 11，55，99.

另外，若完全平方数的个位数是 6，则其十位数是奇数.

因此，完全平方数的末两位不可能是 66.

于是，我们只需找出完全平方数的末两位是 44.

由于$(50k+m)^2=2500k^2+100km+m^2$，则 $50k+m$ 与 m 的平方有相同的末两位数码，因此只要找出在$\{1,2,\cdots,50\}$中，它们的平方的末两位数码是 44 即可.

我们计算 12^2，18^2，22^2，28^2，32^2，38^2，42^2，48^2 可知，只有

$12^2=144$，$38^2=1444$.

于是，具有题设性质的数只有 $50k+12$，$50k+38$，其中 $k\in\{0,1,2,\cdots,19\}$.

所以在不超过 1000 的数的完全平方数的末两位数码相同的数有 40 个.

例 20 （2005 年克罗地亚数学竞赛题）设 P 为整系数多项式，且满足 $P(5)=2005$. 试问：$P(2005)$能否为完全平方数？

解 设 $P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$.

于是，

$P(5)=a_n\cdot 5^n+a_{n-1}\cdot 5^{n-1}+\cdots+a_1\cdot 5+a_0$， ①

$P(2005)=a_n\cdot 2005^n+a_{n-1}\cdot 2005^{n-1}+\cdots+a_1\cdot 2005+a_0$. ②

②－①得

$P(2005)-P(5)=a_n(2005^n-5^n)+a_{n-1}(2005^{n-1}-5^{n-1})+\cdots+a_1(2005-5)$. ③

因为 $2005^k-5^k=2000(2005^{k-1}+2005^{k-2}\times 5+\cdots+2005\times 5^{k-2}+5^{k-1})$，

所以，式③中的各项能被 2000 整除，即

$P(2005)-P(5)=2000A$，其中 A 为整数.

因此，$P(2005)=2000A+2005$，且 $P(2005)$的后两位数为 05.

而 05 不可能为一个完全平方数的后两位，所以，$P(2005)$不可能为完全平方数.

例 21 （1991 年英国数学奥林匹克题）证明：当 n 是非负整数时，$3^n+2\cdot 17^n$ 不是完全平方数.

证明 （1）$n=4m$ 时，

$3^n+2\cdot 17^n=(3^4)^m+2\cdot(17^4)^m=81^m+2\cdot 83521^m$.

此时，$3^n+2\cdot 17^n$ 的个位数是 3，因而不是完全平方数.

（2）$n=4m+1$ 时，

$3^n+2\cdot 17^n=3\cdot(3^4)^m+2\cdot 17\cdot(17^4)^m=3\cdot 81^m+2\cdot 17\cdot 83521^m$.

此时，$3^n+2\cdot17^n$ 的个位数是 7，因而不是完全平方数.

(3) $n=4m+2$ 时，

$3^n+2\cdot17^n=9\cdot81^m+2\cdot289\cdot83521^m$.

此时，$3^n+2\cdot17^n$ 的个位数仍是 7，因而不是完全平方数.

(4) $n=4m+3$ 时，

$3^n+2\cdot17^n=27\cdot81^m+2\cdot4913\cdot83521^m$.

此时，$3^n+2\cdot17^n$ 的个位数也是 3，因而不是完全平方数.

由以上，对非负整数 n，$3^n+2\cdot17^n$ 不是完全平方数.

例 22 （1976 年第 39 届莫斯科数学奥林匹克题）试问：是否存在这样的自然数 A，当把它补在自己的右边，所得的数恰是一个完全平方数？

解 假设 A 是满足条件的 n 位数，则 $\overline{AA}$ 应是一个完全平方数 k^2，则有

$\overline{AA}=A(10^n+1)=k^2$.

显然 10^n+1 应为一个素数平方的倍数.

容易想到，当 n 为奇数时，10^n+1 是 11 的倍数.

可以证明 $10^{11}+1$ 是 $11^2=121$ 的倍数.

事实上，

$10^{11}+1=11(10^{10}-10^9+10^8-10^7+10^6-10^5+10^4-10^3+10^2-10+1)$.

由于当 t 为偶数时，$10^t\equiv1 \pmod{11}$；当 t 为奇数时，$10^t\equiv10 \pmod{11}$.

于是有

$10^{10}-10^9+10^8-10^7+10^6-10^5+10^4-10^3+10^2-10+1$

$\equiv1-10+1-10+1-10+1-10+1-10+1$

$\equiv0 \pmod{11}$.

因而 $10^{11}+1$ 能被 11^2 整除.

但是 $\dfrac{10^{11}+1}{121}=826446281$ 不是一个 11 位数，它的最小平方数倍数是

$16\cdot\dfrac{10^{11}+1}{121}=13223140496$.

这是一个 11 位数.

为此取 $A=13223140496$.

则 $\overline{AA}$ 是一个平方数，它等于 $(4\cdot826446281)^2$.

例 23 （1991 年全国高中联赛题）设 a_n 为下述自然数 N 的个数：N 的各位数字之和为 n 且每位数字只能取 1，3 或 4. 求证：a_{2n} 是完全平方数，这里 $n=1$，2，….

证法 1 设 $N=\overline{x_1x_2\cdots x_k}$，其中 x_1，x_2，…，$x_k\in\{1,3,4\}$，且 $x_1+x_2+\cdots+$

$x_k=n$. 假定 $n>4$. 删去 x_1 时，则当 x_1 依次取 1，3，4 时，$x_2+x_3+\cdots+x_k$ 分别等于 $n-1$，$n-3$，$n-4$. 故 $n>4$ 时，$a_n=a_{n-1}+a_{n-3}+a_{n-4}$.

下面证明 a_{2n} 为完全平方数，且当 $n\geqslant3$ 时，$a_{2n}=(\sqrt{a_{2n-2}}+\sqrt{a_{2n-4}})^2$.

(1) $n=1$，2，3 时，a_{2n} 分别为 1^2，2^2，3^3，易知命题成立；

(2) 假设 $n=1$，2，…，k ($k\geqslant3$) 时命题成立，即 $a_{2k}=(\sqrt{a_{2k-2}}+\sqrt{a_{2k-4}})^2$ 为完全平方数.

当 $n=k+1$ 时，

$$\begin{aligned}a_{2k+2}&=a_{2k+1}+a_{2k-1}+a_{2k-2}\\&=(a_{2k}+a_{2k-2}+a_{2k-3})+a_{2k-1}+a_{2k-2}\\&=a_{2k}+2a_{2k-2}+(a_{2k-1}+a_{2k-3}+a_{2k-4})-a_{2k-4}\\&=2(a_{2k}+a_{2k-2})-a_{2k-4}\\&=2[(\sqrt{a_{2k-2}}+\sqrt{a_{2k-4}})^2+a_{2k-2}]-a_{2k-4}\\&=4a_{2k-2}+a_{2k-4}+4\sqrt{a_{2k-2}}\cdot\sqrt{a_{2k-4}}\\&=(2\sqrt{a_{2k-2}}+\sqrt{a_{2k-4}})^2\\&=[(\sqrt{a_{2k-2}}+\sqrt{a_{2k-4}})+\sqrt{2_{2k-2}}]^2\\&=(\sqrt{a_{2k}}+\sqrt{a_{2k-2}})^2,\text{（由归纳假设）}\end{aligned}$$

即当 $n=k+1$ 时命题也成立.

所以对一切 $n\in\mathbf{N}$，有 a_{2n} 是完全平方数.

证法 2 注意到 n 的首位数字只取 1，3 或 4，若去掉其首位数字，则有递推关系 $a_n=a_{n-1}+a_{n-3}+a_{n-4}$.

易知 $a_1=1$，$a_2=1$，$a_3=2$，$a_4=4$，数列 $\{a_n\}$ 的特征方程为 $x^4-x^3-x-1=0$.

分解因式得

$$(x^2+1)(x^2-x-1)=0. \qquad ①$$

注意到式①左端含有因式 x^2-x-1，而 $x^2-x-1=0$ 正是斐波那契数列 $\{f_n\}$ 的特征方程，其中，

$f_0=f_1=1$，$f_n=f_{n-1}+f_{n-2}$ ($n\geqslant2$).

这使我们想到，数列 $\{a_n\}$ 是否含有斐波那契数列 $\{f_n\}$ 的某种“基因”?

下面将两个数列加以比较：

$a_1=1=f_0f_1$，$a_2=1=f_1^2$，$a_3=2=f_1f_2$，

$a_4=4=f_2^2$，$a_5=6=f_2f_3$，$a_6=9=f_3^2$，

……

由此猜想，一般应有

$a_{2n}=f_n^2,\ a_{2n+1}=f_nf_{n+1}.$ ②

对 n 用数学归纳法.

当 $n=1$，2 时皆已验证.

设式②已对于 n 成立，则在 $n+1$ 时，

$a_{2n+2}=a_{2n+1}+a_{2n-1}+a_{2n-2}=f_nf_{n+1}+f_{n-1}f_n+f_{n-1}^2=f_nf_{n+1}+f_{n-1}f_{n+1}=f_{n+1}^2$；

$a_{2n+3}=a_{2n+2}+a_{2n}+a_{2n-1}=f_{n+1}^2+f_n^2+f_{n-1}f_n=f_{n+1}^2+f_nf_{n+1}=f_{n+1}f_{n+2}.$

因此，对所有正整数 n，式②皆成立.

故结论得证.

注：此解法是由陶平生先生给出的.

3. 关注平方数在特定模下的余数特征

例 24 （1988 年“友谊杯”国际数学竞赛题）证明没有一个自然数 n，使得

$$n^6+3n^5-5n^4-15n^3+4n^2+12n+3$$

的值是某个自然数的平方.

证法 1 $n^6+3n^5-5n^4-15n^3+4n^2+12n+3$

$$=n[n^4(n+3)-5n^2(n+3)+4(n+3)]+3$$
$$=n(n+3)(n^2-1)(n^2-4)+3$$
$$=(n-2)(n-1)n(n+1)(n+2)(n+3)+3.$$

上式的第一项是 6 个连续整数相乘,因此

$4\mid(n-2)(n-1)n(n+1)(n+2)(n+3).$

于是 $n^6+3n^5-5n^4-15n^3+4n^2+12n+3$ 为 $4k+3$ 型的数，因而对所有的自然数 n，均不是平方数.

证法 2 模 4 得

$$n^6+3n^5-9n^4-11n^3+8n^2+12n+3$$
$$\equiv n^6-n^5-n^4+n^3+3$$
$$\equiv n^3(n^3-n^2-n+1)+3$$
$$\equiv n^3[(n+1)(n^2-n+1)-n(n+1)]+3$$
$$\equiv n^3(n+1)(n^2-2n+1)+3$$
$$\equiv n^3(n+1)(n-1)^2+3 \pmod 4.$$

若 $n\equiv 0,2\pmod 4$,则 $n^3\equiv 0\pmod 4$；

若 $n\equiv \pm 1\pmod 4$,则 $(n+1)(n-1)\equiv 0\pmod 4$.

于是，恒有 $n^3(n+1)(n-1)^2\equiv 0\pmod 4$.

故 $n^6+3n^5-9n^4-11n^3+8n^2+12n+3\equiv n^3(n+1)(n-1)^2+3\equiv 3\pmod 4$.

但完全平方数 $x^2\equiv 0$，$1\pmod 4$，所以，$n^6+3n^5-9n^4-11n^3+8n^2+12n+3$ 不

是完全平方数.

例 25 （1982 年第 45 届莫斯科数学奥林匹克题）将数 1，2，…，1982 分别平方后，按某种顺序写成一列，得到一个多位数. 问：这个多位数可能是完全平方数吗？

解 这个多位数不是完全平方数.

我们注意这样一个事实：

若 $3|a$，则 $3|a^2$.

若 $3\nmid a$，则 $a^2\equiv 1 \pmod 3$.

由于 1，2，…，1982 中有 3，6，9，…，1980 共 660 个 3 的倍数，则有 $1982-660=1322$ 个不是 3 的倍数，由于

$1322\equiv 2 \pmod 3$.

所以所得到的多位数是一个被 3 除余 2 的数，因此不可能是完全平方数.

例 26 （1972 年基辅数学奥林匹克题）证明数列 11，111，1111，…中的每一个都不是完全平方数.

证法 1 设 $k^2=\underbrace{11\cdots1}_{t个}$，$t\geqslant 2$，$t\in\mathbf{N}$，则 k 是奇数. 令 $k=2l+1$，则

$(2l+1)^2=\underbrace{11\cdots1}_{t个}$.

$4l^2+4l=\underbrace{11\cdots1}_{(t-1)个}0$.

由于 $11\cdots10$ 不是 4 的倍数，所以上式不可能成立.

于是 $11\cdots1$ 不是完全平方数.

证法 2 由于

$\underbrace{11\cdots111}_{t个}=\underbrace{11\cdots1}_{(t-2)个}00+11$，$t\geqslant 2$，$t\in\mathbf{N}$.

由于 $\underbrace{11\cdots1}_{(t-2)个}00\equiv 0 \pmod 4$，

$11\equiv 3 \pmod 4$.

于是 $\underbrace{11\cdots111}_{t个}\equiv 3 \pmod 4$，$(t\geqslant 2$，$t\in\mathbf{N})$.

由于奇数的平方被 4 除余 1，偶数的平方能被 4 整除，因而 $\underbrace{11\cdots1}_{t个}$ $(t\geqslant 2$，$t\in\mathbf{N})$ 不是完全平方数.

例 27 （第 20 届北欧数学竞赛题）已知正整数数列 $\{a_n\}$ 满足 $a_0=m$，$a_{n+1}=a_n^5+487$ $(n\geqslant 0)$. 试求 m 的值，使得 $\{a_n\}$ 中完全平方数的个数最大.

解 注意到，若 a_n 是一个完全平方数，则

$a_n\equiv 0$ 或 1 (mod 4).

若 $a_k\equiv 0\pmod 4$，则

$$a_{k+i}\equiv\begin{cases}3\pmod 4, & i\text{ 为奇数};\\ 2\pmod 4, & i\text{ 为偶数}.\end{cases}$$

从而，当 $n>k$ 时，a_n 不是完全平方数.

若 $a_k\equiv 1\pmod 4$，则 $a_{k+1}\equiv 0\pmod 4$. 从而，当 $n>k+1$ 时，a_n 不是完全平方数.

于是，数列$\{a_n\}$中至多有两个完全平方数，设为 a_k 和 a_{k+1}.

令 $a_k=s^2$ (s 为奇数)，则 $a_{k+1}=s^{10}+487=t^2$.

设 $t=s^5+r$，则 $t^2=(s^5+r)^2=s^{10}+2s^5r+r^2$.

从而，$2s^5r+r^2=487$. ①

若 $s=1$，则 $r(2+r)=487$，该方程无整数解.

若 $s=3$，则 $486r+r^2=487$，解得 $r=1$，$r=-487$ (舍去).

若 $s>3$，方程①显然无正整数解.

从而，$a_k=9$.

而当 $n>0$ 时，$a_n>487$，故 $m=a_0=9$.

另一方面，当 $a_0=9$ 时，$a_1=9^5+487=244^2$ 是一个完全平方数.

综上所述，所求的 $m=9$.

例 28 (1988 年奥地利-波兰数学竞赛题) 两个整数数列$\{a_k\}_{k\geq 0}$与$\{b_k\}_{k\geq 0}$满足

$b_k=a_k+9, a_{k+1}=8b_k+8, (k\geq 0)$.

又，数 1988 出现于$\{a_k\}_{k\geq 0}$与$\{b_k\}_{k\geq 0}$中.

求证数列$\{a_k\}_{k\geq 0}$不含完全平方数的项.

证明 由已知条件得 $a_{k+1}=8a_k+80$.

由此递推公式可得$\{a_k\}$的通项公式

$$a_k=a_0\cdot 8^k+80\cdot\frac{8^k-1}{7}.$$

当 $k\geq 3$ 时，

$a_k=16[4a_0 8^{k-2}+5(8^{k-1}+8^{k-2}+\cdots+1)]$.

由于对模 8，

$4a_0 8^{k-2}+5(8^{k-1}+8^{k-2}+\cdots+1)\equiv 5\pmod 8$,

因而不是完全平方数.

因此 a_k ($k\geq 3$) 不是完全平方数.

下面验证 a_0，a_1，a_2 都不是完全平方数.

因为 $k\geq 1$ 时，$8|a_k$，且 b_k 是奇数，所以

a_k 与 b_k 均不可能等于 1988.

因此必有 $a_0=1988$ 或 $b_0=1988$.

当 $b_0=1988$ 时，$a_0=1979$.

若 $a_0=1988$，则 $a_1=8\cdot1998$，此时 a_0 与 a_1 均不是平方数，而 $a_2=16[4\cdot1988+5(8+1)]$也不是平方数.

若 $a_0=1979$，则

$a_1=8\cdot1989, a_2=8\cdot(8\cdot1989+10)=16\cdot7961.$

a_0，a_1 和 a_2 均不是平方数.

于是对所有 $k\geqslant0$，a_k 不是完全平方数.

例 29 （IMO-27 试题）设 d 是异于 2，5，13 的任一正整数. 求证：在集合 $\{2,5,13,d\}$ 中可以找到两个不同的元素，使得 $ab-1$ 不是完全平方数.

证法 1 由于 $2\cdot5-1$，$2\cdot13-1$，$5\cdot13-1$ 都是平方数，于是只需证明 $2d-1$，$5d-1$ 和 $13d-1$ 中至少有一个不是完全平方数.

(1) 若 d 是偶数，设 $d=2m$，则 $2d-1=4m-1$ 不是完全平方数.

(2) 若 d 是 $4k+3$ 型的奇数，则 $5d-1=20k+14=4(5k+3)+2$ 不是完全平方数.

(3) 若 d 是 $4k+1$ 型的奇数，则

$13d-1=52k+12=4(13k+3)$，

$5d-1=20k+4=4(5k+1)$.

因此需证明 $13k+3$ 与 $5k+1$ 至少有一个不是完全平方数.

若 $13k+3$ 是完全平方数，则 $13k+3$ 是 $4t$ 或 $4t+1$ 型的数.

若 $13k+3=4t$，则

$5k+1=(13k+3)-8k-2=4t-8k-2=4(t-2k)-2$，

于是 $5k+1$ 不是完全平方数.

若 $13k+3=4t+1$，则

$5k+1=(13k+3)-8k-2=4(t-2k)-1$，

于是 $5k+1$ 也不是完全平方数.

同样可证，若 $5k+1$ 是完全平方数，则 $13k+3$ 不是完全平方数.

综合 (1)、(2)、(3)，$2d-1$，$5d-1$ 和 $13d-1$ 中至少有一个不是完全平方数.

证法 2 假设 $2d-1$，$5d-1$，$13d-1$ 都是完全平方数，设

$2d-1=x^2$，$5d-1=y^2$，$13d-1=z^2$，其中 x，y，z 都是正整数.

由 $2d-1=x^2$ 可知，x 为奇数.

设 $x=2n-1$，于是 $2d-1=(2n-1)^2$，即 $d=2n^2-2n+1$，从而 d 也是奇数.

于是 $5d-1$ 与 $13d-1$ 都是偶数，即 y 与 z 都是偶数.

设 $y=2p$，$z=2q$.

由 $5d-1=y^2$，$13d-1=z^2$，可得

$8d=z^2-y^2=4q^2-4p^2$，即 $2d=q^2-p^2=(q+p)(q-p)$.

由于 $q+p$ 与 $q-p$ 具有相同的奇偶性，则 $(q+p)(q-p)$ 或为奇数，或为 4 的倍数. 然而当 d 为奇数时，$2d$ 不是奇数也不是 4 的倍数，出现矛盾.

因此，$2d-1$，$5d-1$ 和 $13d-1$ 中至少有一个不是完全平方数.

4. 关注平方数序列的间距特征

例 30 （2004 年日本数学奥林匹克题）证明：不存在正整数 n，使得 $2n^2+1$，$3n^2+1$，$6n^2+1$ 全为完全平方数.

证明 若题中结论不真，那么，此三数均为完全平方数，则

$(36n^4+18n^2+1)^2-1=36n^2(6n^2+1)(3n^2+1)(2n^2+1)$

是完全平方数. 但这是不可能的，因为不存在两个正整数的平方差为 1.

例 31 （2008 年国家队集训培训题）一个由正整数组成的无穷等差数列（非常数的）包含了一个项为完全立方数. 求证：这个数列也包含一项，它是完全立方但不是完全平方.

证明 设该无穷等差数列为 $a_1<a_2<\cdots<a_n<\cdots$，公差为 d.

不妨设 a_1 为立方数 a^3，则形如 $(a+md)^3$ 的项都包含在数列 $\{a_n\}$ 中，$m\in\mathbf{N}_+$.

取 $m=a^2d$ 得 $(a+a^2d^2)^3$ 严格在两个相邻的平方数 $(ad)^2$ 和 $(ad+1)^2$ 之间，则不是平方数，于是 $(a+a^2d^2)^3$ 不是平方数. 于是 $a_{(a+a^2d^2)^3-a^3}$ 这一项就是满足要求的项.

例 32 （2004 年斯洛文尼亚国家队选拔赛题）求所有正整数 n，使得 $n\cdot 2^{n-1}+1$ 是完全平方数.

解 设 $n\cdot 2^{n-1}+1=m^2$，即

$$n\cdot 2^{n-1}=(m+1)(m-1). \quad ①$$

显见 $n=1$，$n=2$，$n=3$ 不满足问题的条件.

设 $n>3$，则式①左边的值是偶数，因此，m 一定是奇数.

记 $m=2k+1$，于是，有 $n\cdot 2^{n-3}=k(k+1)$.

因为连续的整数 k 和 $k+1$ 互素，所以，2^{n-3} 恰好被 k 和 $k+1$ 其中之一整除，这意味着 $2^{n-3}\leqslant k+1$.

由此得出

$n\geqslant k$，$2^{n-3}\leqslant n+1$.

后一不等式对 $n=4$ 和 $n=5$ 成立.

用数学归纳法可简便地证明，对于 $n\geqslant 6$，$2^{n-3}>n+1$ 成立.

检验知，$4\times2^3+1=33$ 不是完全平方数，$5\times2^4+1=81$ 是完全平方数.

例 33 是否存在两个自然数 a，b，使得 a^2+2b^2 和 b^2+2a 同时为完全平方数.

证明 结论是否定的. 事实上，当 $a\geqslant b>0$ 时，由 $a^2<a^2+2b^2\leqslant a^2+2a<(a+1)^2$ 可知 a^2+2b 不是完全平方数.

同理，在 $b\geqslant a>0$ 时，$b^2<b^2+2a<(b+1)^2$，即 b^2+2a 也不是完全平方数.

所以，无论 a，b 取何自然数，a^2+2b 与 b^2+2a 不可能同时为完全平方数.

5. 关注平方数的表达式特征

例 34 （1974 年第 35 届美国普特南数学竞赛题）根据下面的定理：一个素数 $p>2$ 当且仅当 $p\equiv1\pmod 4$ 时，能写成两个完全平方数的和（即 $p=m^2+n^2$，m 和 n 是整数）.

求出那些素数，使之能写为下列两种形式之一：

(1) x^2+16y^2；(2) $4x^2+4xy+5y^2$.

这里 x 与 y 是整数，但不一定是正的.

解 (1) 如果 $p\equiv1\pmod 4$，则

$p\equiv1\pmod 8$，或 $p\equiv5\pmod 8$.

若 $p=m^2+n^2$，且 p 是奇数，则 m 和 n 一为奇数，一为偶数.

设 m 为奇数，n 为偶数，且设 $n=2v$，则

$p=m^2+4v^2$，且 $m^2\equiv1\pmod 8$.

由 $p\equiv1\pmod 8$ 可得 v 为偶数. 设 $v=2w$，则

$p=m^2+16w^2$.

反之，若 $p=m^2+16w^2$ 成立，则

$p\equiv m^2\pmod 8$.

于是对于素数 $p\equiv1\pmod 8$，可以写成 x^2+16y^2 的形式.

(2) 由 (1)，对于奇素数 p，有 $p=m^2+4v^2$.

若 $p\equiv5\pmod 8$，则 v 是奇数.

于是 m 可写成

$m=2u+v$.

$p=(2u+v)^2+4v^2=4u^2+4uv+5v^2$.

反之，若 $p=4u^2+4uv+5v^2$，并且 p 是奇数，则有

$p=(2u+v)^2+4v^2$.

于是 $2u+v$ 是奇数，即 v 是奇数，从而 $p\equiv5\pmod 8$.

于是对于素数 $p\equiv5\pmod 8$，可以写成 $4x^2+4xy+5y^2$.

例 35 （2004 年西部数学奥林匹克题）求所有的整数 n，使得 $n^4+6n^3+11n^2+$

$3n+31$ 是完全平方数.

解 设 $A=n^4+6n^3+11n^2+3n+31$ 是完全平方数，即 $A=(n^2+3n+1)^2-3(n-10)$ 是完全平方数.

当 $n>10$ 时，$A<(n^2+3n+1)^2$，所以 $A\leqslant(n^2+3n)^2$，则

$(n^2+3n+1)^2-(n^2+3n)^2\leqslant 3n-30$，即 $2n^2+3n+31\leqslant 0$，这不可能.

当 $n=10$ 时，$A=(10^2+3\times10+1)^2=131^2$ 是完全平方数.

当 $n<10$ 时，$A>(n^2+3n+1)^2$.

若 $n\leqslant-3$，或 $10>n\geqslant0$，则 $n^2+3n\geqslant0$. 于是

$A\geqslant(n^2+3n+2)^2$，

$2n^2+9n-27\leqslant0$，

$$-7\leqslant\frac{-3(\sqrt{33}+3)}{4}\leqslant n\leqslant\frac{3(\sqrt{33}-3)}{4}<3.$$

所以 $n=-6$，-5，-4，-3，0，1，2，此时对应的 $A=409$，166，67，40，31，52，145 都不是完全平方数.

若 $n=-2$，-1 时，与之对应的 $A=37$，34 也都不是完全平方数.

所以，只有当 $n=10$ 时，A 是完全平方数.

例 36 （2005 年斯洛文尼亚国家队选拔考试题）求所有正整数对 (m,n)，使得 m^2-4n 和 n^2-4m 均为完全平方数.

解 显然，$m^2-4n<m^2$.

若 $m^2-4n=(m-1)^2$，则 $2m-1=4n$，矛盾.

故 $m^2-4n\leqslant(m-2)^2$，得 $4m\leqslant4n+4$，即 $m\leqslant n+1$.

同理，$n\leqslant m+1$.

故 $n-1\leqslant m\leqslant n+1$.

(1) 若 $m=n-1$，则

$n^2-4m=n^2-4(n-1)=(n-2)^2$，

$m^2-4n=m^2-4(m+1)=(m-2)^2-8=t^2\ (t\in\mathbf{N}_+)$.

从而，$(m-2+t)(m-2-t)=8$.

故 $\begin{cases}m-2+t=4,\\m-2-t=2,\end{cases}$ 解得 $m-2=3$.

所以，$m=5$，$n=6$，满足要求.

(2) 若 $m=n$，则

$m^2-4n=n^2-4m=m^2-4m=(m-2)^2-4=t^2\ (t\in\mathbf{N})$.

从而 $(m-2+t)(m-2-t)=4$，解得 $m-2=2$.

所以，$m=n=4$，满足要求.

(3) 若 $m=n+1$，则

$m^2-4n=(n+1)^2-4n=(n-1)^2$，

$n^2-4m=n^2-4(n+1)=(n-2)^2-8=t^2(t\in\mathbf{N}_+)$，

从而，$(n-2+t)(n-2-t)=8$，

解得 $n-2=3$.

所以，$n=5$，$m=6$，满足要求.

综上，所求正整数对 $(m,n)=(4,4),(5,6),(6,5)$.

例 37 （2006 年泰国数学奥林匹克题）求所有的素数 p，使得 $\frac{2^{p-1}-1}{p}$ 为完全平方数.

解 对每个素数 p，设

$f(p)=\frac{2^{p-1}-1}{p}$.

下面证明：当 $p>7$ 时，$f(p)$ 不是完全平方数.

假设存在素数 $p>7$ 满足 $2^{p-1}-1=pm^2$（m 为整数），则 m 必为奇数.

分两种情况进行讨论.

(1) $p=4k+1$ $(k>1)$，

则 $2^{4k}-1=(4k+1)m^2\equiv1\pmod 4$.

但 $2^{4k}-1\equiv3\pmod 4$，矛盾.

(2) $p=4k+3$ $(k>1)$，

则 $2^{4k+2}-1=(2^{2k+1}-1)(2^{2k+1}+1)=pm^2$.

考虑到 $(2^{2k+1}-1,2^{2k+1}+1)=1$，再分两种情况讨论.

(i) 设 $2^{2k+1}-1=u^2$，$2^{2k+1}+1=pv^2$.

由于 $k>1$，则 $2^{2k+1}+1\equiv1\pmod 4$.

但 $pv^2\equiv3\times1\equiv3\pmod 4$，矛盾.

(ii) 设 $2^{2k+1}-1=pu^2$，$2^{2k+1}+1=v^2$，则

$2^{2k+1}=v^2-1=(v-1)(v+1)$.

因此，$v-1=2^s$，$v+1=2^t(s<t)$.

注意到 $2^{t-s}=\frac{v+1}{v-1}-1+\frac{2}{v-1}$，则 $(v-1)\mid2$.

故 $v=2$ 或 $v=3$.

当 $v=2$ 时，$2^{2k+1}+1=4$，矛盾；

当 $v=3$ 时，$2^{2k+1}=8$，$k=1$，与 $k>1$ 的假设矛盾.

综上，当 $p>7$ 时，$f(p)$不是完全平方数.

再用枚举法对 $p=2$，3，5，7 的情况进行验证，知 $p=3$ 和 $p=7$ 时满足题意.

例 38 （2005 年白俄罗斯数学奥林匹克题）(1) 是否存在正整数 a，b 使得对任何正整数 n，数 2na+5^nb 是完全平方数?

(2) 是否存在正整数 a，b，c 使得对任何正整数 n，数 2na+5^nb+c 是完全平方数?

解 (1) 不存在；(2) 不存在.

(1) 用反证法.

设存在 a，b 满足题目要求，即存在正整数数列$\{x_n\}$使得

$x_n^2=2^na+5^nb$ $(n\geqslant 0)$.

令 $a=5^kc$，其中，k $(k\geqslant 0)$ 是整数，c 不是 5 的倍数.

当 $n>k$ 时，$x_n^2=5^k(2^nc+5^{n-k}b)$.

因为 $2^nc+5^{n-k}b$ 不含 5 的因子，而 x_n^2 是完全平方数，所以，$k=2m$，m $(m\geqslant 0)$ 为整数.

引理 对于 $n>k$，数$\left(\frac{x_n}{5^m}\right)^2=\frac{x_n^2}{5^k}=2^nc+5^{n-k}b$ 是完全平方数，即$\frac{x_n}{5^m}$是整数.

引理的证明：由于$\frac{x_n}{5^m}$是有理数，设$\frac{x_n}{5^m}=\frac{p}{q}$，其中，$(p,q)=1$.

若 $q>1$，因为$(p^2,q^2)=1$，所以，$\left(\frac{x_n}{5^m}\right)^2$ 不是整数，矛盾. 因此，$q=1$，$\frac{x_n}{5^m}$是整数.

下面证明原题.

考虑数列$\{y_n\}$，$y_n=\frac{x_n}{5^m}$，其中，$n>2m$.

注意到 $y_n^2\equiv 2^nc$ (mod 5)，所以，

$y_{n+1}^2\equiv 2y_n^2$ (mod 5).

显然，$\{y_{n+1}^2(\text{mod } 5),n=0,1,2,\cdots\}=\{1,4\}$.

当 $y_n^2\equiv 1$ (mod 5) 时，$y_{n+1}^2\equiv 2\times 1=2$ (mod 5)；

当 $y_n^2\equiv 4$ (mod 5) 时，$y_{n+1}^2=2\times 4\equiv 3$ (mod 5)，矛盾.

因此，不存在满足要求的 a，b.

(2) 假设命题成立，即存在正整数 a，b，c 和正整数数列$\{x_n\}$使得

$x_n^2=2^na+5^nb+c$ $(n\geqslant 1)$.

注意到

$25x_n^2=25\times 2^na+5^{n+2}b+25c>2^{n+2}a+5^{n+2}b+c=x_{n+2}^2$.

从而，$5x_n>x_{n+2}$.

所以，$x_{n+2}\leqslant 5x_n-1$.

两边平方得 $x_{n+2}^2\leqslant 25x_n^2-10x_n+1$. 于是，

$$\begin{aligned}10x_n&\leqslant 25x_n^2+1-x_{n+2}^2\\&=21\times 2^n a+24c+1+(4\times 2^n a+5^{n+2}b+c)-x_{n+2}^2\\&=21\times 2^n a+24c+1.\end{aligned}$$

从而，$\frac{10x_n}{2^n}\leqslant 21a+\frac{24c}{2^n}+\frac{1}{2^n}$.

当 $n\to\infty$ 时，$\frac{10x_n}{2^n}\leqslant 21a$，但

$$\lim_{n\to\infty}\left(\frac{10x_n}{2^n}\right)^2=\lim_{n\to\infty}\frac{100(2^n a+5^n b+c)}{4^n}=\lim_{n\to\infty}100b\times\left(\frac{5}{4}\right)^n\to\infty,$$ 矛盾.

例 39 （2004 年克罗地区数学竞赛题）证明：任意五个相邻的正整数的平方和不是一个正整数的平方.

证明 记 5 个相邻正整数分别为 $n-2$，$n-1$，n，$n+1$，$n+2$，它们的平方和等于 $(n-2)^2+(n-1)^2+n^2+(n+1)^2+(n+2)^2=5(n^2+2)$，显然能被 5 整除. 故只有当它能被 25 整除，即 n^2+2 能被 5 整除时，它才能是一个正整数的平方. 但平方数 n^2 除以 5 不能得到余数 3.

例 40 证明：任意连续 5 个正整数的积不是完全平方数.

证明 设 5 个连续正整数为 $a-2$，$a-1$，a，$a+1$，$a+2$ $(a>2)$，则

$N=(a-2)(a-1)a(a+1)(a+2)=a(a^2-1)(a^2-4)=a(a^4-5a^2+4)$.

假定 N 是完全平方数，对于 a 的任意一个奇素因数 p，如果 $p\mid(a-2)$，则

$p\ [a-(a-2)]=2$，与 p 是奇素数矛盾.

于是，p 不整除 $a-2$.

同理，p 不整除 $a+2$.

类似地，p 不整除 $a\pm1$.

因此，p 与 a^4-5a^2+4 互素.

因为 p 是完全平方数 N 的因数，p 在 N 中的指数为偶数，所以，p 在 a 中的指数为偶数.

这表明，除 2 以外，a 的素因数 p 在 a 中的指数都为偶数，故 $a=2m^2$ 或 $a=m^2$.

如果 $a=m^2$，则 a 为完全平方数.

又 $N=a(a^4-5a^2+4)$ 为完全平方数，则 a^4-5a^2+4 为完全平方数. 这与

$(a^2-3)^2<a^4-5a^2+4<(a^2-2)^2$

矛盾. 因此，$a=2m^2$.

故 $N=(a-2)(a-1)a(a+1)(a+2)$

$$=(2m^2-2)(2m^2-1)2m^2\cdot(2m^2+1)(2m^2+2)$$

$$=(2m)^2 2(m^2-1)(m^2+1)\cdot(2m^2-1)(2m^2+1).$$

因为 N，$(2m)^2$ 都是完全平方数，所以，$N'=2(m^2-1)(m^2+1)(2m^2-1)(2m^2+1)$是完全平方数.

从而，$(m^2-1)(m^2+1)(2m^2-1)(2m^2+1)$为偶数.

但$(2m^2-1)(2m^2+1)$是奇数，所以，$(m^2-1)(m^2+1)$是偶数. 从而，m 是奇数，即 $m\equiv1 \pmod 2$.

如果 $m\equiv0 \pmod 3$，则

$$N'=2(m^2-1)(m^2+1)(2m^2-1)(2m^2+1)$$

$$\equiv2\times(-1)\times1\times(-1)\times1\equiv2 \pmod 3,$$

与 N'是完全平方数矛盾.

所以，$m\equiv1,2 \pmod 3$.

由 $m\equiv1 \pmod 2$，得 $m\equiv1,3,5 \pmod 6$.

由 $m\equiv1,2 \pmod 3$，得 $m\equiv1,2,4,5 \pmod 6$.

所以，$m\equiv1,5 \pmod 6$.

令 $m=6t\pm1$，则 $m^2=36t^2\pm12t+1=12k+1$.

故 $N'=2(m^2-1)(m^2+1)(2m^2-1)(2m^2+1)$

$$=2\times12k(12k+2)(24k+1)(24k+3)$$

$$=144k(6k+1)(24k+1)(8k+1).$$

所以，$k(6k+1)(24k+1)(8k+1)$为完全平方数.

但 k，$6k+1$，$24k+1$，$8k+1$ 两两互素，因此，k，$6k+1$，$24k+1$，$8k+1$ 都是完全平方数.

因为 $6k+1$，$24k+1$ 是完全平方数，所以，$4(6k+1)$，$24k+1$ 是完全平方数，即 $24k+4$，$24k+1$ 是完全平方数.

令 $24k+4=x^2$，$24k+1=y^2$，则

$$3=24k+4-(24k+1)=x^2-y^2\geqslant3.$$

因为不等式等号成立，所以，

$y=1$，$x=2$，$k=0$.

从而，$m=\pm1$，$a=2$，与 $a>2$ 矛盾.

故 N 不是完全平方数.

6. 善于将问题转化处理

例 41 （2004 年国家队集训测试题）已知数列$\{c_n\}$满足：$c_0=1$，$c_1=0$，$c_2=$

$2005, c_{n+2}=-3c_n-4c_{n-1}+2008(n=1,2,3,\cdots)$. 记 $a_n=5(c_{n+2}-c_n)(502-c_{n-1}-c_{n-2})+4^n\times2004\times501(n=2,3,\cdots)$. 问:对 $n>2$, a_n 是否均为平方数? 说明理由.

解 由 $c_{n+2}-c_n=-4(c_n+c_{n-1})+2008$ 知

$a_n=-20(c_n+c_{n-1}-502)(502-c_{n-1}-c_{n-2})+4^{n+1}\times501^2$.

令 $d_n=c_n-251$, 则

$d_{n+2}=-3d_n-4d_{n-1}(n=1,2,3,\cdots)$,

$d_0=-250$,

$d_1=-251$,

$d_2=1754$.

$a_n=20(d_n+d_{n-1})(d_{n-1}+d_{n-2})+4^{n+1}\times501^2(n=2,3,\cdots)$.

令 $w_n=d_n+d_{n-1}$, 则

$w_{n+2}=w_{n+1}-4w_n, w_1=-501, w_2=1503$,

$a_n=20w_nw_{n-1}+4^{n+1}\times501^2$.

令 $w_n=501T_n$, 则

$T_{n+2}=T_{n+1}-4T_n, T_1=-1, T_2=3$.

定义 $T_0=-1$, 则

$a_n=501^2\times2^2(5T_nT_{n-1}+4^n)$.

设 $x^2-x+4=0$ 的两个根为 α、β,则

$\alpha+\beta=1$, $\alpha\beta=4$,

$T_n-\alpha T_{n-1}=\beta(T_{n-1}-\alpha T_{n-2})=\cdots=\beta^{n-1}(T_1-\alpha T_0)=-\beta^{n-1}(\alpha-1)$,

$T_n-\beta T_{n-1}=-\alpha^{n-1}(\beta-1)$.

故$(T_n-\alpha T_{n-1})(T_n-\beta T_{n-1})=(\alpha\beta)^{n-1}(\alpha-1)(\beta-1)=4^n$,即

$T_n^2-T_nT_{n-1}+4T_{n-1}^2=4^n$.

所以 $a_n=501^2\times2^2(5T_nT_{n-1}+T_n^2-T_nT_{n-1}+4T_{n-1}^2)=1002^2(T_n+2T_{n-1})^2$.

例 42 (2005 年全国高中联赛题)数列$\{a_n\}$满足:$a_0=1, a_{n+1}=\dfrac{7a_n+\sqrt{45a_n^2-36}}{2}$, $n\in\mathbf{N}$. 证明:

(1) 对任意 $n\in\mathbf{N}$, a_n 为正整数.

(2) 对任意 $n\in\mathbf{N}$, $a_na_{n+1}-1$ 为完全平方数.

证明 (1) 由题设得 $a_1=5$, 且$\{a_n\}$严格单调递增. 将条件式变形得

$2a_{n+1}-7a_n=\sqrt{45a_n^2-36}$,

两边平方整理得 $a_{n+1}^2-7a_na_{n+1}+a_n^2+9=0$, ①

所以 $a_n^2-7a_{n-1}a_n+a_{n-1}^2+9=0$, ②

①－②得 $(a_{n+1}-a_{n-1})(a_{n+1}+a_{n-1}-7a_n)=0$.

因为 $a_{n+1}>a_n$，所以 $a_{n+1}+a_{n-1}-7a_n=0$，故

$$a_{n+1}=7a_n-a_{n-1}. \quad ③$$

由③式及 $a_0=1$，$a_1=5$ 可知，对任意 $n\in\mathbf{N}$，a_n 为正整数.

(2) 将①两边配方，得 $(a_{n+1}+a_n)^2=9(a_na_{n+1}-1)$，所以

$$a_na_{n+1}-1=\left(\frac{a_{n+1}+a_n}{3}\right)^2. \quad ④$$

由③得 $a_{n+1}+a_n=9a_n-(a_n+a_{n-1})$，所以

$$a_{n+1}+a_n\equiv-(a_n+a_{n-1})\equiv\cdots\equiv(-1)^n(a_1+a_0)\equiv0 \pmod 3.$$

因此，$\frac{a_{n+1}+a_n}{3}$ 为整数，所以 $a_na_{n+1}-1$ 是完全平方数.

例 43 （第 18 届爱尔兰数学奥林匹克题）已知奇数 m，n 满足 m^2-n^2+1 整除 n^2-1. 证明：m^2-n^2+1 是一个完全平方数.

证明 先证明两个引理.

引理 1 设 p，k 是给定的正整数，$p\geqslant k$，k 不是完全平方数，则关于 a，b 的不定方程

$$a^2-pab+b^2-k=0 \quad ①$$

无正整数解.

引理 1 的证明：假设有正整数解，设 (a_0,b_0) 是使 $a+b$ 最小的一组正整数解，且 $a_0\geqslant b_0$，又设 $a_0'=pb_0-a_0$，则 a_0，a_0' 是关于 t 的一元二次方程

$$t^2-pb_0t+b_0^2-k=0 \quad ②$$

的两根.

所以，$a_0'^2-pa_0'b_0+b_0^2-k=0$.

若 $0<a_0'<a_0$，则 (b_0,a_0') 也是方程①的一组正整数解，且 $b_0+a_0'<a_0+b_0$，矛盾. 所以，$a_0'\leqslant0$ 或 $a_0'\geqslant a_0$.

(1) 若 $a_0'=0$，则 $a_0=pb_0$，代入方程①得 $b_0^2-k=0$. 但 k 不是完全平方数，矛盾.

(2) 若 $a_0'<0$，则 $a_0>pb_0$. 从而，$a_0\geqslant pb_0+1$.

故
$$\begin{aligned}a_0^2-pa_0b_0+b_0^2-k&=a_0(a_0-pb_0)+b_0^2-k\\&\geqslant a_0+b_0^2-k\geqslant pb_0+1+b_0^2-k\\&>p-k\geqslant0,\end{aligned}$$

矛盾.

(3) 若 $a_0'\geqslant a_0$，因为 a_0，a_0' 是方程②的两根，由韦达定理得 $a_0a_0'=b_0^2-k$. 但 $a_0a_0'\geqslant a_0^2\geqslant b_0^2>b_0^2-k$，矛盾.

综上，方程①无正整数解.

引理 2　设 p，k 是给定的正整数，$p\geqslant 4k$，则关于 a，b 的不定方程

$$a^2-pab+b^2+k=0 \quad ③$$

无正整数解.

引理 2 的证明：假设有正整数解，设 (a_0,b_0) 是使 $a+b$ 最小的一组正整数解，且 $a_0\geqslant b_0$，又设 $a_0'=pb_0-a_0$，则 a_0，a_0' 是关于 t 的一元二次方程

$$t^2-pb_0t+b_0^2+k=0 \quad ④$$

的两根.

所以，$a_0'^2-pa_0'b_0+b_0^2+k=0$.

若 $0<a_0'<a_0$，则 (b_0,a_0') 也是方程③的一组正整数解，且 $b_0+a_0'<a_0+b_0$，矛盾.

所以，$a_0'\leqslant 0$ 或 $a_0'\geqslant a_0$.

(1) 若 $a_0'\leqslant 0$，则 $a_0\geqslant pb_0$，故 $a_0^2-pa_0b_0+b_0^2+k\geqslant b_0^2+k>0$，矛盾.

(2) 若 $a_0'\geqslant a_0$，则 $a_0\leqslant\frac{pb_0}{2}$. 因为方程④的两根是 $\frac{pb_0\pm\sqrt{(pb_0)^2-4(b_0^2+k)}}{2}$，则

$$a_0=\frac{pb_0-\sqrt{(pb_0)^2-4(b_0^2+k)}}{2}.$$

又因为 $a_0\geqslant b_0$，则

$$b_0\leqslant\frac{pb_0-\sqrt{(pb_0)^2-4(b_0^2+k)}}{2}$$

$$\Rightarrow(p-2)b_0\geqslant\sqrt{p^2b_0^2-4b_0^2-4k}$$

$$\Rightarrow(p-2)^2b_0^2\geqslant p^2b_0^2-4b_0^2-4k$$

$$\Rightarrow(4p-8)b_0^2\leqslant 4k.$$

而 $p\geqslant 4k\geqslant 4$，则 $(4p-8)b_0^2\geqslant 4p-8\geqslant 2p>4k$，矛盾.

综上所述，方程③无正整数解.

下面证明原题.

不妨设 m，$n>0$.

因为 $(m^2-n^2+1)\mid(n^2-1)$，则

$(m^2-n^2+1)\mid[(n^2-1)+(m^2-n^2+1)]=m^2$.

(1) 若 $m=n$，则 $m^2-n^2+1=1$ 是完全平方数.

(2) 若 $m>n$，因为 m，n 都是奇数，则 $2\mid(m+n)$，$2\mid(m-n)$.

设 $m+n=2a$，$m-n=2b$，则 a，b 都是正整数.

因为 $m^2-n^2+1=4ab+1$，$m^2=(a+b)^2$，则

$(4ab+1)\mid(a+b)^2$.

设$(a+b)^2=k(4ab+1)$，其中k是正整数，则

$a^2-(4k-2)ab+b^2-k=0$.

若k不是完全平方数，由引理1，矛盾.

所以，k是完全平方数.

故$m^2-n^2+1=4ab+1=\dfrac{(a+b)^2}{k}=\left(\dfrac{a+b}{\sqrt{k}}\right)^2$也是完全平方数.

(3) 若$m<n$，因为m，n都是奇数，则$2\mid(m+n)$，$2\mid(m-n)$.

设$m+n=2a$，$n-m=2b$，则a，b都是正整数.

因为$m^2-n^2+1=-(4ab-1)$，$m^2=(a-b)^2$，则

$(4ab-1)\mid(a-b)^2$.

设$(a-b)^2=k(4ab-1)$，其中k是正整数，则

$a^2-(4k+2)ab+b^2+k=0$.

由引理2，矛盾.

综上所述，m^2-n^2+1是完全平方数.

例44 （2002—2003年度匈牙利数学奥林匹克决赛题）设n是大于2的整数，a_n是最大的n位数，且既不是两个完全平方数的和，又不是两个完全平方数的差.

(1) 求a_n（表示成n的函数）.

(2) 求n的最小值，使得a_n的各位数字的平方和是一个完全平方数.

解 (1) $a_n=10^n-2$.

先证最大性.

在n位十进制整数中，只有$10^n-1>10^n-2$.

但$10^n-1=9\times\dfrac{10^n-1}{9}$

$$=\left(\frac{9+\frac{10^n-1}{9}}{2}+\frac{\frac{10^n-1}{9}-9}{2}\right)\left(\frac{9+\frac{10^n-1}{9}}{2}-\frac{\frac{10^n-1}{9}-9}{2}\right)$$

$$=\left(\frac{9+\frac{10^n-1}{9}}{2}\right)^2-\left(\frac{\frac{10^n-1}{9}-9}{2}\right)^2.$$

因为$\dfrac{10^n-1}{9}$为奇数，所以，10^n-1可表示为两个完全平方数的差. 这与题设矛盾.

下面证10^n-2满足条件.

若10^n-2可表示为两个完全平方数的差，则它模4余0，1或3. 但$10^n-2\equiv$

$2 \pmod 4$，所以，10^n-2 不能表示为两个完全平方数的差.

若 10^n-2 可表示为两个完全平方数的和，则它或被 4 整除，或模 8 余 2. 但 10^n-2 不能被 4 整除且模 8 余 6（因为 $n>2$）.

所以，10^n-2 不能表示为两个完全平方数的和.

(2) 由 $9^2(n-1)+64=k^2$，得

$9^2(n-1)=(k-8)(k+8)$.

因为 $n\geqslant 3$，且 $-8\not\equiv 8 \pmod 9$，所以

$81\mid(k-8)$ 或 $81\mid(k+8)$.

若 $81\mid(k-8)$，则 $k_{\min}=89$，$n=98$.

若 $81\mid(k+8)$，则 $k_{\min}=73$，$n=66$.

因此，$n_{\min}=66$.

例 45 （1994 年美国数学奥林匹克题）求最小的正整数 $n>1$，使得 1^2，2^2，3^2，…，n^2 的算术平均数是一个完全平方数.

解 设 $\dfrac{1^2+2^2+\cdots+n^2}{n}=k^2$，其中 $k\in\mathbf{N}$，则

$$\frac{1}{6}(n+1)(2n+1)=k^2. \qquad ①$$

因为 $n\geqslant 2$，所以 $\dfrac{1}{6}(n+1)(2n+1)\geqslant\dfrac{5}{2}$，从而

$k^2\geqslant\dfrac{5}{2}$，$k\geqslant 2$.

因为 $2n+1$ 是奇数，所以由①知，n 必为奇数，令 $n=2m-1$，$m\geqslant 2$，代入①得

$$\frac{1}{3}m(4m-1)=k^2. \qquad ②$$

因此 m 是 3 的倍数或者 $4m-1$ 是 3 的倍数.

若 m 是 3 的倍数，则令 $m=3t$，$t\in\mathbf{N}$，代入②得

$t(12t-1)=k^2$.

由于 t 与 $12t-1$ 互素，因此 t 与 $12t-1$ 都是完全平方数.

但 $12t-1\equiv 3 \pmod 4$，这与“完全平方数除以 4 只能余 0 或 1”矛盾. 所以必有 $4m-1=3t$（$t\in\mathbf{N}$），代入②得

$\dfrac{1}{4}(3t+1)t=k^2$，即

$$(3t+1)t=(2k)^2. \qquad ③$$

因为 $m=\dfrac{1}{4}(3t+1)$，所以 $3t+1$ 是 4 的倍数，从而 t 除以 4 的余数必为 1.

令 $t=4j+1(j\in\mathbf{N})$（因 $m\geqslant2$，故 $t\geqslant3$，从而有 $j\geqslant1$），代入③，得

$(3j+1)(4j+1)=k^2$.

由于 $(4j+1)-(3j+1)=j$，而 $4j+1$ 与 j 互素，因此 $4j+1$ 与 $3j+1$ 互素，从而 $4j+1$ 与 $3j+1$ 都是完全平方数. 令

$$\begin{cases}3j+1=a^2,\\4j+1=b^2,\end{cases} \quad ④$$

其中 a 是不小于 2 的正整数，b 是不小于 3 的奇数. 由上式，得

$3b^2+1=4a^2$.

令 $b=2s+1$，$s\in\mathbf{N}$，代入上式，得

$12s(s+1)+4=4a^2$，即 $3s(s+1)+1=a^2$.

因为 $s(s+1)$ 必为偶数，所以 a 为奇数，且 $a\geqslant3$.

于是，令 $b=4c\pm1$，$a=4d\pm1$，这里 c，$d\in\mathbf{N}$，代入④，得

$3(4c\pm1)^2+1=4(4d\pm1)^2$，

展开，并化简，有

$3c(2c\pm1)=4d(2d\pm1)$.

由上式可知，c 是 4 的倍数. 于是令

$c=4e$，$e\in\mathbf{N}$，

因此，$b=4c\pm1=16e\pm1$.

由 $4j+1=b^2$ 得

$j=\dfrac{b^2-1}{4}=\dfrac{(16e\pm1)^2-1}{4}=8e(8e\pm1)$，于是

$t=4j+1=32e(8e\pm1)+1$，所以

$m=\dfrac{1}{4}(3t+1)=24e(8e\pm1)+1$，从而有

$n=2m-1=48e(8e\pm1)+1$，显然

$n\geqslant48\times1\times(8\times1-1)+1=337$.

容易验证，$n=337$ 时，

$$\frac{1^2+2^2+\cdots+n^2}{n}=\frac{1}{6}(n+1)(2n+1)=\frac{1}{6}\times338\times675=169\times225=(13\times15)^2.$$

综上所述，可知所求的最小的小于 1 的正整数 n 为 337.

例 46 （2003 年保加利亚国家数学奥林匹克题）给定一个序列：$y_1=y_2=1$，$y_{n+2}=(4k-5)y_{n+1}-y_n+4-2k$，$n\geqslant1$. 求满足以下条件的所有整数 k：它使序列的每一项都是一个完全平方数.

解 设 k 满足题中的条件.

由已知可得

$y_3=2k-2$，$y_4=8k^2-20k+13$.

由于 y_3 是个偶数，则存在一个整数 $a\geqslant 0$，使得 $2k-2=4a^2$，则 $k=2a^2+1$，即 $k\geqslant 1$.

于是，$y_4=32a^4-8a^2+1$.

当 $a=0$ 时，$k=1$.

当 $a>0$ 时，设 b ($b\geqslant 0$) 是一个整数，且满足 $y_4=b^2$.

于是，$16a^4-8a^2+1+16a^4=b^2$，即 $(4a^2-1)^2+(4a^2)^2=b^2$.

由于 $4a^2-1$ 与 $4a^2$ 互素，所以，$4a^2-1$，$4a^2$，b 是一组本原勾股数. 因此，存在着互素的正整数 m，n，使得

$$\begin{cases}4a^2-1=n^2-m^2, & ①\\ 4a^2=2mn, & ②\\ b=n^2+m^2. & ③\end{cases}$$

由①，②得

$n^2-m^2+1=2mn$，即

$$(n+m)^2-2n^2=1. \qquad ④$$

由②得 $nm=2a^2$. 又由于 m，n 互素，故 m，n 具有不同的奇偶性. 但 m 不能是偶数，否则，将推出 $n^2\equiv -1 \pmod 4$，这是不可能的.

因此，m 是奇数，n 是偶数.

于是，存在一个整数 $t\geqslant 0$，使得 $n=2t^2$.

再利用式④得

$2n^2=8t^4=(n+m-1)(n+m+1)$.

所以，$2t^4=\dfrac{n+m-1}{2}\cdot\dfrac{n+m+1}{2}=u(u+1)$，其中 u，$u+1$ 是相继的两个整数. 由于它们是互素的，故可以推出，一个是某个整数的 4 次幂(c^4)，另一个是某数的 4 次幂的 2 倍($2d^4$). 于是，

$c^4-2d^4=\pm 1$.

如果 $c^4-2d^4=1$，则

$d^8+2d^4+1=d^8+c^4$，即 $(d^4+1)^2=(d^2)^4+c^4$.

上式具有 $x^4+y^4=z^2$ 的形式，已经证明它没有满足 $xyz\neq 0$ 的整数解. 故 $c=\pm 1$，$d=0$.

所以，$u=0$，有 $t=0$. 因此，$n=a=0$. 矛盾.

如果 $c^4-2d^4=-1$，则

$1-2d^4+d^8=d^8-c^4$，即 $(d^2)^4-c^4=(d^4-1)^2$.

上式具有 $x^4-y^4=z^2$ 的形式，它也没有满足 $xyz\neq 0$ 的整数解. 于是，$d=\pm 1$，$c=\pm 1$.

对于 u，仅有的新值是 $u=1$，因此，$t^4=1$，$n^2=4$，$n=2$，$m=1$，$a^2=1$，以及 $k=3$.

从而，找到了关于 k 的仅有的选择：$k=1$ 和 $k=3$.

当 $k=1$ 时，我们得到一个周期序列：1，1，0，1，1，0，…，它满足题目中的约束条件.

当 $k=3$ 时，序列是：

$y_1=y_2=1$，$y_{n+2}=7y_{n+1}-y_n-2$.

由于 $y_3=4=2^2$，$y_4=25=5^2$，$y_5=169=13^2$，我们假设它是奇数项的斐波那契数的平方.

如果 $\{u_n\}$ 是斐波那契数列，易知，$u_{n+2}=3u_n-u_{n-2}$，以及 $u_{n+2}u_{n-2}-u_n^2=1$ 对奇数 n 成立.

故 $(u_{n+2}+u_{n-2})^2=9u_n^2$.

因此，$u_{n+2}^2=9u_n^2-u_{n-2}^2-2u_{n+2}u_{n-2}=7u_n^2-u_{n-2}^2-2$.

这就确认了我们的假设.

故 $k=1$ 和 $k=3$.

【模拟实战】

1. (2004 年全国高中联赛题) 设 p 是给定的奇素数，正整数 k 使得 $\sqrt{k^2-pk}$ 也是一个正整数，则 $k=$________.
2. (2006 年泰国数学奥林匹克题) 求所有的整数 n，使得 $n^2+59n+881$ 为完全平方数.
3. (2007 年克罗地亚数学竞赛题) 求使 $n^2+2007n$ 为完全平方数的自然数 n 的最大值.
4. (2005 年克罗地亚数学奥林匹克题) 求所有使 $2^4+2^7+2^n$ 为完全平方数的正整数 n.
5. (第 18 届爱尔兰数学奥林匹克题) 证明：2005^{2005} 是两个完全平方数的和，不是两个完全立方数的和.
6. (2004 年西班牙数学奥林匹克题) 求所有的两位正数 a，b，使 $100a+b$ 和 $201a+b$ 均为四位数，且均为完全平方数.
7. (2007 年波罗的海地区数学竞赛题) 设正整数 a，b 满足 $b<a$，且 $ab(a-b)\mid(a^3+b^3+ab)$. 证明：ab 是完全立方数.

8. (2007年克罗地亚数学竞赛题) 已知 p 为大于3的素数. 证明: p 的平方被24除的余数为1.
9. (2005年新西兰数学奥林匹克题) 求所有满足等式 $k^2+l^2+m^2=2^n$ 的整数解 (k, l, m, n).
10. (第7届巴尔干地区数学奥林匹克题) 设 n 是一个正整数, A 是一个 $2n$ 位数, 且每位上的数均为4, B 是一个 n 位数, 且每位上的数均为8. 证明: $A+2B+4$ 是一个完全平方数.
11. (第31届俄罗斯数学奥林匹克题) 在不超过 10^{20} 的完全平方数中, 是其倒数第17位数为7的数多, 还是其倒数第17位数为8的数多?
12. (第18届韩国数学奥林匹克题) 求所有的正整数 n, 它能唯一地表示为5个或少于5个正整数的平方和 (这里, 两个求和顺序不同的表达式被认为是相同的, 如 3^2+4^2 和 4^2+3^2 被认为是25的同一个表达式).
13. (1989年第52届莫斯科数学奥林匹克题) 求满足下列条件的一切自然数 x: x 的各位数字之积等于 $44x-86868$, 而各位数字之和是完全立方数.
14. 设 a 为素数, b 为正整数, 且 $9(2a+b)^2=509(4a+511b)$, 求 a, b 的值.
15. (2008年国家队集训培训题) 设 n 为正整数, 求证: 数 n^7+7 不是一个完全平方数.
16. 如果一个完全平方数可以写成一个素数与另一个完全平方数的和, 则称其为"好平方数"; 如果一个完全平方数不能写成一个素数与另一个完全平方数的和, 则称其为"坏平方数". 求证: 好平方数与坏平方数都有无数个.
17. (第19届亚太地区数学奥林匹克题) 已知集合 S 由9个最大素因子不超过3的整数组成. 求证: S 中存在3个互不相同的元素, 它们的乘积是一个完全立方数.
18. 每一个正整数 a 遵循下面的过程得到数 $d=d(a)$.

    (1) 将 a 的最后一位数字移到第一位得到数 b;

    (2) 将 b 平方得到数 c;

    (3) 将 c 的第一位数字移到最后一位得到数 d.

    例如, $a=2003$, $b=3200$, $c=10240000$, $d=02400001=2400001=d(2003)$.

    求所有的正整数 a, 使得 $d(a)=a^2$.

第九章 公约数和公倍数

【基础知识】

1. 公约数和最大公约数

(1) 若 $c \mid a_1$，$c \mid a_2$，…，$c \mid a_n$，则 c 叫 a_1，a_2，…，a_n 的公约数.

a_1，a_2，…，a_n 的所有公约数中最大的一个叫 a_1，a_2，…，a_n 的最大公约数，记作 $(a_1, a_2, \cdots, a_n)$.

(2) 若 a_1，a_2，…，a_n 的标准分解式为

$$a_1=\prod_{i=1}^{m} p_i^{\alpha_i},\ a_2=\prod_{i=1}^{m} p_i^{\beta_i},\ \cdots,\ a_n=\prod_{i=1}^{m} p_i^{\delta_i}.$$

其中 p_i 为素数，α_i，β_i，…，δ_i 为非负整数，$i=1, 2, \cdots, m$. 则

$$(a_1,a_2,\cdots,a_n)=\prod_{i=1}^{m} p_i^{t_i},$$

其中 $t_i=\min\{\alpha_i, \beta_i, \cdots, \delta_i\}$.

(3) 如果 a 是 b 的倍数，那么 a 和 b 的公约数的集合与 b 的约数集合相等.

(4) 如果 a 是 b 的倍数，则 $(a, b)=b$.

(5) 设 a 和 b 是不同时等于 0 的整数，且 $d=ax_0+by_0$ 是形如 $ax+by$(x,y 是整数)的数中的最小正数，则 $d=(a,b)$.

(6) 数 a 和 b 的公约数集合与它的最大公约数的约数集合相等.

(7) 设 m 是任意正整数，则 $(am,bm)=(a,b)m$.

(8) 设 n 是 a 和 b 的一个公约数，则 $\left(\frac{a}{n},\frac{b}{n}\right)=\frac{(a,b)}{n}$.

(9) 设正整数 a 和 b($a>b$)满足等式 $a=bq+r$，$0\leqslant r<b$，则 $(a,b)=(b,r)$.

由此可得到求 a，b 最大公约数的辗转相除法：

由 $a=bq_1+r_1$，$0\leqslant r_1<b$，

若 $r_1=0$，则 $(a,b)=b$；

若 $r_1\neq 0$，则又可用 r_1 去除 b，得 $b=r_1q_2+r_2$，$0\leqslant r_2<r_1$.

若 $r_2=0$，则 $(a,b)=(b,r_1)=r_1$；

若 $r_2\neq 0$，再用 r_2 去除 r_1，得 $r_1=r_2q_3+r_3$，$0\leqslant r_3<r_2$.

如果继续下去，由于 $b>r_1>r_2>r_3>\cdots$ 以及 $r_i(i=1,2,\cdots)$ 是非负整数，则一定在进行到某一次时，例如第 $n+1$ 次，得到 $r_{n+1}=0$，但由于 $r_n\neq0$，则有

$(a,b)=(b,r_1)=(r_1,r_2)=\cdots=(r_{n-1},r_n)=r_n$.

用此法还可以求 (5) 中形如 $ax+by$ 的最小正数 $d=ax_0+by_0$.

2. 公倍数和最小公倍数

(1) 若 $a_1\mid b$，$a_2\mid b$，…，$a_n\mid b$，则 b 叫 a_1，a_2，…，a_n 的公倍数.

a_1，a_2，…，a_n 的所有公倍数中最小的一个叫 a_1，a_2，…，a_n 的最小公倍数，记作 $[a_1, a_2, \cdots, a_n]$.

(2) 若 a_1，a_2，…，a_n 的标准分解式为

$$a_1=\prod_{i=1}^{m}p_i^{\alpha_i},\ a_2=\prod_{i=1}^{m}p_i^{\beta_i},\ \cdots,\ a_n=\prod_{i=1}^{m}p_i^{\delta_i}.$$

其中 p_i 为素数，α_i，β_i，…，δ_i 为非负整数，$i=1$，2，…，m. 则

$$[a_1,a_2,\cdots,a_n]=\prod_{i=1}^{m}p_i^{r_i},$$

其中 $r_i=\max\{\alpha_i,\beta_i,\cdots,\delta_i\}$.

(3) a_1，a_2，…，a_n 的最小公倍数是它们的任一公倍数的约数.

(4) $[a,b]=\dfrac{ab}{(a,b)}$.

【典型例题与基本方法】

例 1 （第 19 届意大利数学奥林匹克题）设 n 是一个三位数，满足 $100\leqslant n\leqslant 999$. 求所有的 n，使得 n^3 的末三位数等于 n.

解 原命题等价于 $1000\mid(n^2-n)=n(n-1)$.

由于 $(n,n-1)=1$，且仅有一个是偶数，又 $1000=2^3\times5^3$，所以，有以下 4 种情况：

(1) n 是 1000 的倍数，则 n 不是三位数.

(2) $n-1$ 是 1000 的倍数，则 n 不是三位数.

(3) n 是 2^3 的倍数，$n-1$ 是 5^3 的倍数. 设 $n=2^3a$，$n-1=5^3b$，则 $2^3a-5^3b=1$. 由辗转相除法易知 $a=47$，$b=3$，即 $n=376$ 满足条件.

(4) n 是 5^3 的倍数，$n-1$ 是 2^3 的倍数. 同理，设 $n=5^3c$，$n-1=2^3d$，由 $5^3c-2^3d=1$，得 $c=5$，$d=78$，$n=625$.

例 2 （2003—2004 年度匈牙利数学奥林匹克题）设 c，d 是整数. 证明：存在无穷多个不同的整数对 $(x_n,y_n)(n=1,2,\cdots)$，使得 x_n 是 cy_n+d 的一个约数，且 y_n 是 cx_n+d 的一个约数的充分必要条件为 c 是 d 的一个约数.

证明 充分性.

因为 $c\mid d$，记 $d=kc(k\in\mathbf{Z})$，

所以，$x_i=i,y_i=-(i+k),i=1,2,3,\cdots$ 即为满足条件的无穷多个整数对.

必要性.

假设 $c\nmid d$，则 $d\neq0$.

若 $c=0$，由于 d 有限大，显然，不存在无限多个整数整除 d，矛盾.

若 $c\neq0$，存在无穷多个不同的整数对 $(x_n,y_n)(n=1,2,\cdots)$，使得 $y_n\mid(cx_n+d)$，$x_n\mid(cy_n+d)$.

由于整数对的无限性，因此，其中必然存在一个数的绝对值大于 c^4d^4.

不妨设 $|x_1|>c^4d^4$.

因为 $x_1\mid(cy_1+d)$，所以，

$|cy_1+d|\geqslant|x_1|>c^4d^4$.

故 $|cy_1|\geqslant c^4d^4-|d|$.

又 $|c|>1$，所以，

$|cy_1|\geqslant2c^3d^4-|d|,|y_1|>c^2d^4$，

$\dfrac{(cy_1+d)(cx_1+d)}{x_1y_1}=c^2+\dfrac{cd}{x_1}+\dfrac{cd}{y_1}+\dfrac{d^2}{x_1y_1}$.

由 $\left|\dfrac{cd}{x_1}+\dfrac{cd}{y_1}+\dfrac{d^2}{x_1y_1}\right|\leqslant\dfrac{1}{|c|^3}+\dfrac{1}{|c|}+\dfrac{1}{|c^6|}<\dfrac{1}{2^3}+\dfrac{1}{2}+\dfrac{1}{2^6}<1$，

且 $\dfrac{(cy_1+d)(cx_1+d)}{x_1y_1}\in\mathbf{Z}$，

因此，$\dfrac{(cy_1+d)(cx_1+d)}{x_1y_1}=c^2$.

因为 $c\nmid d$，故必存在一个素数 p 和正整数 α，使 $p^\alpha\mid c$ 且 $p^\alpha\nmid d$.

因为 $p^{2\alpha}\mid c^2$，所以，$\dfrac{cy_1+d}{x_1}$ 和 $\dfrac{cx_1+d}{y_1}$ 两个整数中必有一个含 p 的幂次不小于 α.

不妨设 $p^\alpha x_1\mid(cy_1+d)$.

而 $p^\alpha\mid c$，$p^\alpha\nmid d$，矛盾.

因此，$c\mid d$.

例3 已知两数中，每一个除以它们的最大公约数所得的商之和等于 18，它们的最小公倍数等于 975，求这两个正整数.

解 设两个正整数为 x，y，且 $d=(x,y)$，则

$x=dx_1,y=dy_1,(x_1,y_1)=1$.

于是 $[x,y]=\dfrac{xy}{d}=dx_1y_1$.

由题意，有

$$\begin{cases}x_1+y_1=18,\\ dx_1y_1=975.\end{cases}$$

显然 $x_1\leqslant 17$，$y_1\leqslant 17$，又

$975=1\cdot 3\cdot 5\cdot 5\cdot 13.$

又由 x_1，y_1 一定是 975 的约数，则只能有

$x_1=5$，$y_1=13$，$d=15$.

因此 $x=75$，$y=195$.

例 4 （1972 年第 1 届美国数学奥林匹克题）设记号$(a,b,\cdots,g)$和$[a,b,\cdots,g]$分别表示正整数 $a,b,\cdots,g$ 的最大公约数和最小公倍数，例如$(3,6,9)=3$，$[6,15]=30$.

证明$\dfrac{[a,b,c]^2}{[a,b][b,c][c,a]}=\dfrac{(a,b,c)^2}{(a,b)(b,c)(c,a)}$.

证法 1 设 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$，$c=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_n^{\gamma_n}$，其中 p_i 是素数，α_i，β_i，γ_i 是非负整数，$i=1$，2，…，n.

由最大公约数和最小公倍数的定义可得

$$[a,b]=\prod_{i=1}^{n}p_i^{\max(\alpha_i,\beta_i)},(a,b)=\prod_{i=1}^{n}p_i^{\min(\alpha_i,\beta_i)},$$

其中 $\max(\alpha_i,\beta_i)$表示 α_i,β_i 中较大者，$\min(\alpha_i,\beta_i)$表示 α_i,β_i 中较小者.

于是本题相当于证明

$$\begin{aligned}&2\max(\alpha_i,\beta_i,\gamma_i)-\max(\alpha_i,\beta_i)-\max(\beta_i,\gamma_i)-\max(\gamma_i,\alpha_i)\\=&2\min(\alpha_i,\beta_i,\gamma_i)-\min(\alpha_i,\beta_i)-\min(\beta_i,\gamma_i)-\min(\gamma_i,\alpha_i).\end{aligned}$$

不失一般性，令 $\alpha_i\leqslant\beta_i\leqslant\gamma_i$，对任意的 i 都成立$(i=1,2,\cdots,n)$，则

$$\begin{aligned}&2\max(\alpha_i,\beta_i,\gamma_i)-\max(\alpha_i,\beta_i)-\max(\beta_i,\gamma_i)-\max(\gamma_i,\alpha_i)\\=&2\gamma_i-\beta_i-\gamma_i-\gamma_i=-\beta_i,\end{aligned}$$

$$\begin{aligned}&2\min(\alpha_i,\beta_i,\gamma_i)-\min(\alpha_i,\beta_i)-\min(\beta_i,\gamma_i)-\min(\gamma_i,\alpha_i)\\=&2\alpha_i-\alpha_i-\beta_i-\alpha_i=-\beta_i.\end{aligned}$$

于是欲证的等式成立.

从而本题得证.

证法 2 利用公倍数和最小公倍数的结论（4），有

$$[a,b]=\frac{ab}{(a,b)},[a,b,c]=\frac{abc(a,b,c)}{(a,b)(b,c)(c,a)}.$$

可得 $$\frac{[a,b,c]^2}{[a,b][b,c][c,a]}=\frac{\left\{\dfrac{abc(a,b,c)}{(a,b)(b,c)(c,a)}\right\}^2}{\dfrac{ab}{(a,b)}\cdot\dfrac{bc}{(b,c)}\cdot\dfrac{ca}{(c,a)}}=\frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}.$$

例 5 （1990 年国家集训队培训题）设 a_1，a_2，a_3，…，a_n 都是大于等于 A 的正整数，对于任意的 i，j，$1\leqslant i$，$j\leqslant n$，有 $(a_i,a_j)\leqslant B$. 证明

$$[a_1,a_2,\cdots,a_n]\geqslant\max_{1\leqslant i\leqslant n}\frac{A^i}{B^{\frac{i(i-1)}{2}}},A,B\in\mathbf{N}.$$

记号 (a_i,a_j) 表示 a_i 和 a_j 的最大公约数，$[a_1,a_2,\cdots,a_n]$ 表示 $a_1,a_2,\cdots,a_n$ 的最小公倍数.

证明 用数学归纳法.

(1) $n=1$，2 时，结论显然成立.

(2) 假设 $n=k$ 时结论成立，即

$$[a_1,a_2,\cdots,a_k]\geqslant\max_{1\leqslant i\leqslant k}\frac{A^i}{B^{\frac{i(i-1)}{2}}}.$$

那么，当 $n=k+1$ 时，由 $a_{k+1}\geqslant A$，有

$$\begin{aligned}[a_1,a_2,\cdots,a_k,a_{k+1}]&=[[a_1,a_2,\cdots,a_k],a_{k+1}]\\&=\frac{[a_1,a_2,\cdots,a_k]\cdot a_{k+1}}{([a_1,a_2,\cdots,a_k],a_{k+1})}\\&\geqslant\max_{1\leqslant i\leqslant k}\frac{A^i}{B^{\frac{i(i-1)}{2}}}\cdot\frac{a_{k+1}}{([a_1,a_2,\cdots,a_k],a_{k+1})}\\&\geqslant\max_{1\leqslant i\leqslant k}\frac{A^i}{B^{\frac{i(i-1)}{2}}}.\end{aligned}\qquad ①$$

这里，最后一步用到 $a_{k+1}\geqslant([a_1,a_2,\cdots,a_k],a_{k+1})$.

另一方面，由 $([a_1,a_2,\cdots,a_k],a_{k+1})\leqslant\prod_{i=1}^{k}(a_i,a_{k+1})\leqslant B^k$ 及 $a_{k+1}\geqslant A$，则有

$$\begin{aligned}[a_1,a_2,\cdots,a_k,a_{k+1}]&=\frac{[a_1,a_2,\cdots,a_k]\cdot a_{k+1}}{([a_1,a_2,\cdots,a_k],a_{k+1})}\\&\geqslant\frac{A^k\cdot a_{k+1}}{B^{\frac{k(k-1)}{2}}([a_1,a_2,\cdots,a_k],a_{k+1})}\\&\geqslant\frac{A^k\cdot A}{B^{\frac{k(k-1)}{2}}\cdot B^k}\\&=\frac{A^{k+1}}{B^{\frac{k(k+1)}{2}}}.\end{aligned}\qquad ②$$

由①，②得

$$[a_1,a_2,\cdots,a_k,a_{k+1}]\geqslant\max_{1\leqslant i\leqslant k+1}\frac{A^i}{B^{\frac{i(i-1)}{2}}}.$$

于是 $n=k+1$ 时，结论成立.

从而对所有自然数 n，结论成立.

例 6 （2007 年女子数学奥林匹克题）设 m 为正整数，如果存在某个正整数 n，使得 m 可以表示为 n 和 n 的正约数个数（包括 1 和自身）的商，则称 m 是好数. 求证：

(1) 1，2，…，17 都是好数；

(2) 18 不是好数.

证明 记 $d(n)$ 为正整数 n 的正约数的个数.

(1) 因为 $p=\frac{8p}{d(8p)}, p=3,5,7,11,13,17$，又

$1=\frac{2}{d(2)}, 2=\frac{8}{d(8)}, 4=\frac{36}{d(36)}, 6=\frac{72}{d(72)}, 8=\frac{96}{d(96)}, 9=\frac{108}{d(108)},$

$10=\frac{180}{d(180)}, 12=\frac{240}{d(240)}, 14=\frac{252}{d(252)}, 15=\frac{360}{d(360)}, 16=\frac{128}{d(128)},$

所以 1，2，…，17 都是好数.

(2) 假设存在正整数 n，使得

$$\frac{n}{d(n)}=18, \qquad ①$$

则可设 $n=2^{\alpha_0}3^{\beta_0}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，其中 p_i 是大于 3 的相异素数，$\alpha_0\geqslant 1$，$\beta_0\geqslant 2$，$\alpha_i(i=1,2,\cdots,k)\geqslant 1$.

令 $\alpha_0-1=a, \beta_0-2=b$，显然 $a\geqslant 0, b\geqslant 0$. 由①，得

$$2^a3^bp_1^{\alpha_1}\cdots p_k^{\alpha_k}=(a+2)(b+3)(\alpha_1+1)\cdots(\alpha_k+1). \qquad ②$$

由于对任意素数 p_i 都有

$$p_i^{\alpha_i}\geqslant \alpha_i+1. \qquad ③$$

由②、③可知

$(a+2)(b+3)\geqslant 2^a3^b$.

如果 $b\geqslant 3$，则 $3^b>3(b+3)$. 而 $a\geqslant 0$ 时，$2^a\geqslant\frac{1}{2}(a+2)$，所以

$a^a3^b>\frac{3}{2}(a+2)(b+3)$，矛盾. 故 $b\leqslant 2$.

所以 $b=2$，$a=0$；$b=1$，$a=0$，1，2；$b=0$，$a=0$，1，2，3，4.

(i) 当 $b=2$，$a=0$ 时，式②为

$3^2p_1^{\alpha_1}\cdots p_k^{\alpha_k}=10(\alpha_1+1)\cdots(\alpha_k+1)$，

显然不成立.

(ii) 当 $b=1$，$a=0$，1，2 时，式②为

$3\cdot 2^2p_1^{\alpha_1}\cdots p_k^{\alpha_k}=2^2(a+2)(\alpha_1+1)\cdots(\alpha_k+1)$，

显然不成立.

(iii) 当 $b=0$，$a=0$，1，2，3，4 时，式②为

$$2^a p_1^{a_1}\cdots p_k^{a_k}=3(a+2)(a_1+1)\cdots(a_k+1),$$

也不成立.

综上所述，18 不是好数.

例 7 （2006 年国家集训队选拔赛题）对正整数 M，如果存在整数 a，b，c，d，使得 $M\leqslant a<b\leqslant c<d\leqslant M+49$，$ad=bc$，则称 M 为好数，否则称 M 为坏数. 试求最大的好数和最小的坏数.

解 最大的好数是 576，最小的坏数是 443.

引理 若正整数 a，b，c，d 满足 $a<b\leqslant c<d$，$ad=bc$，则存在正整数 u，v，使得 $a\leqslant(u-1)(v-1)<uv\leqslant d$. 从而（不妨设 $u\leqslant v$）

$$a\leqslant(u-1)(v-1)<(u-1)v\leqslant u(v-1)<uv\leqslant d.$$

引理的证明：由 $ad=bc$ 知 $\frac{a}{(a,c)}\frac{d}{(b,d)}=\frac{b}{(b,d)}\frac{c}{(a,c)}$.

因为 $\left(\frac{a}{(a,c)},\frac{c}{(a,c)}\right)=1$，$\left(\frac{d}{(b,d)},\frac{b}{(b,d)}\right)=1$，故

$$\frac{a}{(a,c)}=\frac{b}{(b,d)}=s,\frac{d}{(b,d)}=\frac{c}{(a,c)}=t.$$

因此 $a=(a,c)s$，$b=(b,d)s$，$c=(a,c)t$，$d=(b,d)t$.

由 $a<b$ 知 $(a,c)<(b,d)$，由 $a<c$ 知 $s<t$.

令 $u=(b,d)$，$v=t$，则

$$a=(a,c)s\leqslant(u-1)(v-1),d=uv.$$

引理得证.

(1) 576 是最大的好数.

由 $576=24\times24<24\times25=24\times25<25\times25=625$，知 576 为好数.

设 $M\geqslant577$，若 M 为好数，则由引理知存在正整数 u，v，$u\leqslant v$，使得

$$M\leqslant(u-1)(v-1)<uv\leqslant M+49.$$

由此知 $uv-(u-1)(v-1)\leqslant49$，即 $u+v\leqslant50$.

另一方面，由 $577\leqslant M\leqslant(u-1)(v-1)\leqslant\left(\frac{u+v-2}{2}\right)^2$ 知

$(u+v-2)^2\geqslant2308>48^2$，从而 $u+v-2\geqslant49$，即 $u+v\geqslant51$，矛盾.

所以 576 为最大的好数.

(2) 当 $1\leqslant M\leqslant288$ 时，取整数 n，使得

$$13n\leqslant M+49<13(n+1),$$ 则

$$13n\leqslant M+49\leqslant337,$$ 从而 $n\leqslant25$.

这样 $12(n-1)=13(n+1)-n-25\geqslant M+50-n-25\geqslant M$，即

$M\leqslant 12(n-1)<13n\leqslant M+49$.

因此对于 $1\leqslant M\leqslant 288$，$M$ 为好数.

取

$$\{(u_i,v_i)\}_{i=1}^{23}=\{(13,26),(14,25),(19,19),(14,26),(15,25),(19,20),(15,26),(20,20),(17,24),(19,22),(20,21),(13,33),(18,24),(20,20),(21,21),(15,30),(19,24),(16,29),(18,26),(19,25),(20,24),(21,23),(14,35)\}.$$

验证知

$u_iv_i\leqslant(u_{i-1}-1)(v_{i-1}-1)+50, i=2,3,\cdots,23$.

$(u_1-1)(v_1-1)=300, u_1v_1=338, (u_{23}-1)(v_{23}-1)=442$.

当 $288<M\leqslant 300$ 时，$M\leqslant(u_1-1)(v_1-1)<u_1v_1\leqslant M+49$.

当 $(u_{i-1}-1)(v_{i-1}-1)<M\leqslant(u_i-1)(v_i-1)$ 时，

$M\leqslant(u_i-1)(v_i-1)<u_iv_i\leqslant(u_{i-1}-1)(v_{i-1}-1)+50\leqslant M+49, i=2,3,\cdots,23$.

因此，当 $288\leqslant M\leqslant 442$ 时，M 为好数.

下证 443 为坏数.

假设 443 为好数，则由引理知存在正整数 $u,v,u\leqslant v$，使得

$443\leqslant(u-1)(v-1)<uv\leqslant 492$.

因此 $uv-(u-1)(v-1)\leqslant 49$，即 $u+v\leqslant 50$.

又 $443\leqslant(u-1)(v-1)\leqslant\left(\frac{u+v-2}{2}\right)^2$，得 $u+v\geqslant 45$.

由 $443\leqslant(u-1)(v-1)=uv-u-v+1\leqslant uv-2\sqrt{uv}+1=(\sqrt{uv}-1)^2$ 知

$\sqrt{uv}\geqslant 22, uv\geqslant 484$. $uv=484,485,486,487,488,489,490,491,492$ 中满足 $45\leqslant u+v\leqslant 50$ 的只有 $(u,v)=(14,35),(18,27)$. 而 $13\times 34=442$，$17\times 26=442$ 与 $(u-1)(v-1)\geqslant 443$ 矛盾. 所以 443 为最小的坏数.

例 8 （CMO-22 试题）试证明：(1) 若 $2n-1$ 为素数，则对于任意 n 个互不相同的正整数 a_1，a_2，…，a_n，都存在 i，$j\in\{1,2,\cdots,n\}$，使得

$$\frac{a_i+a_j}{(a_i,a_j)}\geqslant 2n-1;$$

(2) 若 $2n-1$ 为合数，则存在 n 个互不相同的正整数 a_1，a_2，…，a_n，使得对任意 i，$j\in\{1,2,\cdots,n\}$，都有

$$\frac{a_i+a_j}{(a_i,a_j)}<2n-1,$$

其中 (x,y) 表示正整数 x,y 的最大公约数.

证明 (1) 记 $2n-1$ 为素数 p，不妨设$(a_1,a_2,\cdots,a_n)=1$. 若存在 $i(1\leqslant i\leqslant n)$，使得 $p|a_i$，必然存在 $j\neq i$ 使得 $p\nmid a_j$. 由于 $p\nmid(a_j,a_j)$，则有

$$\frac{a_i+a_j}{(a_i,a_j)}\geqslant\frac{a_i}{(a_i,a_j)}\geqslant p=2n-1.$$

以下只需要考虑$(a_i,p)=1$，$i=1,2,\cdots,n$，则对任意 $i\neq j$ 都是 $p\nmid(a_i,a_j)$. 将 $1,2,\cdots,p-1$ 分成 $n-1$ 类：$\{1,p-1\},\{2,p-2\},\cdots,\{n-1,n\}$. 由抽屉原理可知存在 $i\neq j$，使得 $a_i\equiv a_j\pmod p$ 或者 $a_i+a_j\equiv 0\pmod p$.

当 $a_i\equiv a_j\pmod p$ 时，

$$\frac{a_i+a_j}{(a_i,a_j)}>\frac{a_i-a_j}{(a_i,a_j)}\geqslant p=2n-1;$$

当 $a_i+a_j\equiv 0\pmod p$ 时，

$$\frac{a_i+a_j}{(a_i,a_j)}\geqslant p=2n-1.$$

故 (1) 得证.

(2) 以下我们来构造命题存在性的例子. 由于 $2n-1$ 为合数，则存在两个大于 1 的正整数 p，q 使得 $2n-1=pq$. 可以构造如下 n 个数：

$$a_1=1,\ a_2=2,\ \cdots,\ a_p=p,\ a_{p+1}=p+1,\ a_{p+2}=p+3,\ \cdots,\ a_n=pq-p,$$

其中前面为 p 个连续的整数，从 $p+1$ 至 $pq-p$ 为 $n-p$ 个连续的偶数.

当 $1\leqslant i\leqslant j\leqslant p$ 时，显然有

$$\frac{a_i+a_j}{(a_i,a_j)}\leqslant a_i+a_j\leqslant 2p<2n-1.$$

当 $p+1\leqslant i\leqslant j\leqslant n$ 时，因为 $2|(a_i,a_j)$，所以有

$$\frac{a_i+a_j}{(a_i,a_j)}\leqslant\frac{a_i+a_j}{2}\leqslant pq-p<2n-1.$$

当 $1\leqslant i\leqslant p$，$p+1\leqslant j\leqslant n$ 时，分两种情况：

(i) 当 $i\neq p$ 或 $j\neq n$ 时，显然有

$$\frac{a_i+a_j}{(a_i,\ a_j)}\leqslant pq-1<2n-1;$$

(ii) 当 $i=p$ 且 $j=n$ 时，由于$(p,pq-p)=p$，则有

$$\frac{a_p+a_n}{(a_p,a_n)}\leqslant\frac{pq}{p}\leqslant q<2n-1.$$

经过如上验证，可以看出所构造的几个数满足条件.

例 9 (2007 年国家队培训题) 求证：当 $l\geqslant 2$，$4\leqslant k\leqslant n-4$ 时，方程 $C_n^k=m^l$ 没有整数解.

证明 不妨设 $n\geqslant 2k$，反设原方程有整数解(n,k).

由西勒维斯特(Sylvester)定理，存在素数 $p>k$ 使 $p\mid C_n^k$，因此，$p^l\mid C_n^k$，故 $p^l\mid \prod_{i=1}^{k}(n-i+1)$. 而 $p>k$，故 $n,n-1,\cdots,n-k+1$ 中仅能有一个作为 p 的倍数.

设 $p^l\mid n-i_0, i_0\in\{0,1,2,\cdots,k-1\}$，则

$$n\geqslant n-i_0\geqslant p^l>k^l\geqslant k^2. \quad ①$$

又设 $n-i=a_im_i^l$，其中 a_i 不含 l 次方因子，$m_i\in\mathbf{N}^*$，$i=0,1,2,\cdots,k-1$，则 a_i 的素因子不大于 k.

首先证明，对于 $\forall i\neq j$，均有 $a_i\neq a_j$.

反设存在 $i\neq j$，使得 $a_i=a_j$，则由于 $n-i>n-j$，故

$$m_i>m_j，\ m_i\geqslant m_j+1,$$

$$\begin{aligned}k>j\geqslant j-i&=(n-i)-(n-j)=a_j(m_i^l-m_j^l)\\&\geqslant a_j[(m_j+1)^l-m_j^l]>a_jlm_j^{l-1}\geqslant l\sqrt{a_jm_j^l}\\&\geqslant l\sqrt{n-k+1}\geqslant l\sqrt{\frac{n}{2}+1}>\sqrt{n},\end{aligned}$$

与①矛盾.

进一步，我们再证 $\{a_0,a_1,\cdots,a_{k-1}\}=\{1,2,\cdots,k\}$. 由于 $a_1,a_2,\cdots,a_{k-1}$ 互不相同，因而，转证 $\prod_{i=0}^{k-1}a_i\mid k!$.

将 $n-i=a_im_i^l$ 代入原方程可得

$$\left(\prod_{i=0}^{k-1}a_i\right)\left(\prod_{i=0}^{k-1}m_i\right)^l=k!\ m^l,$$

两边同时约去 $\prod_{i=0}^{k-1}m_i$ 与 m 的最大公约数 d，得

$$\left(\prod_{i=0}^{k-1}a_i\right)u^l=k!\ v^l, \quad ②$$

其中 $u=\dfrac{\prod_{i=0}^{k-1}m_i}{d}, v=\dfrac{m}{d}, (u,v)=1$.

只需证明 $v=1$. 若 $v\neq1$，则 v 有素因子 p_0，此素因子 p_0 也是 $\prod_{i=0}^{k-1}a_i$ 的一个素因子，故 $p_0\leqslant k$. 下面我们来估计 $\prod_{i=0}^{k-1}a_i$ 中含 p_0 的幂次.

对于 $i\in\mathbf{N}^*$，设 $b_1<b_2<\cdots<b_s$ 为 $n,n-1,\cdots,n-k+1$ 中 p_0^i 的倍数，则 $b_s=b_1+(s-1)p_0^i,(s-1)p_0^i=b_s-b_1\leqslant n-(n-k+1)=k-1$，故

$$s\leqslant\left[\frac{k-1}{p_0^i}\right]+1\leqslant\left[\frac{k}{p_0^i}\right]+1.$$

因此，对于 $i\in\mathbf{N}^*$，p_0^i 的倍数在 $n,n-1,\cdots,n-k+1$ 中至多出现 $\left[\frac{k}{p_0^i}\right]+1$ 次，当然在 $a_0,a_1,\cdots,a_{k-1}$ 也是如此，故 $\prod\limits_{i=0}^{k-1}a_i$ 中含 p_0 的幂次至多是 $\sum\limits_{i=1}^{l-1}\left(\left[\frac{k}{p_0^i}\right]+1\right)$（注意，$a_i$ 不含 l 次方因子），而 $k!$ 中含 p_0 的幂次为 $\sum\limits_{i=1}^{\infty}\left[\frac{k}{p_0^i}\right]$，在②式两边比较 p_0 的幂次可知 v^l 中的 p_0 的幂次至多为

$$\sum_{i=1}^{l-1}\left(\left[\frac{k}{p_0^i}\right]+1\right)-\sum_{i=1}^{\infty}\left[\frac{k}{p_0^i}\right]\leqslant l-1,$$

矛盾！故 v 不含素因子，即 $v=1$，所以 $\prod\limits_{i=0}^{k-1}a_i\mid k!$，这样我们有 $\{a_0,a_1,\cdots,a_{k-1}\}=\{1,2,\cdots,k\}$.

最后我们来导出一个矛盾.

由于 $k\geqslant4$，利用刚得到的结论，存在 i_1，i_2，i_3 使得 $a_{i_j}=2^{j-1}(j=1,2,3)$，故

$n-i_1=m_{i_1}^l,n-i_2=2m_{i_2}^l,n-i_3=4m_{i_3}^l$.

我们指出 $(n-i_2)^2\neq(n-i_1)(n-i_3)$，否则设

$b=n-i_2,x=b-(n-i_1),y=-b+(n-i_3),0<|x|<|y|<k$.

由 $(b-x)(b+y)=b^2$ 得 $(y-x)b=xy$，显然有 $x\neq y$，则

$|xy|=b|x-y|\geqslant b>n-k>(k-1)^2\geqslant|xy|$，矛盾.

因此，$(n-i_2)^2\neq(n-i_1)(n-i_3)$，即 $m_{i_2}^2\neq m_{i_1}m_{i_3}$.

不妨设 $m_{i_2}^2\neq m_{i_1}m_{i_3}$，我们有

$$\begin{aligned}2(k-1)n&>n^2-(n-k+1)^2>(n-i_2)^2-(n-i_1)(n-i_3)\\&=4(m_{i_2}^l)^2-4(m_{i_1}m_{i_3})^l\geqslant4(m_{i_1}m_{i_3}+1)^l-4(m_{i_1}m_{i_3})^l\geqslant4(m_{i_1}m_{i_3})^{l-1}.\end{aligned}$$

若 $l=2$，则 $a_{i_3}=4$ 有平方因子，故 $l\geqslant3$，此时有

$$\begin{aligned}2(k-1)nm_{i_1}m_{i_3}&>4l(m_{i_1}m_{i_3})^l=l(n-i_1)(n-i_2)\\&>l(n-k+1)^2>3\left(n-\frac{n}{6}\right)^2>2n^2.\end{aligned}$$

由 $m_{i_j}\leqslant n^{\frac{1}{l}}\leqslant n^{\frac{1}{3}},j=1,2,3$ 得

$kn^{\frac{2}{3}}\geqslant km_{i_1}m_{i_3}>(k-1)m_{i_1}m_{i_3}>n$，于是 $k>n^{\frac{1}{3}}$，这与①中 $n>k^2$ 矛盾！

至此，我们证得反设错误，故本题结论成立.

【解题思维策略分析】

1. 灵活应用倍数的性质处理问题

例 10 （IMO－43 预选题）已知正整数 m，$n\geqslant 2$，a_1，a_2，…，a_n 是整数，且其中任何一个都不是 m^{n-1} 的倍数．证明：存在不全为零的整数 e_1，e_2，…，e_n，使 $e_1a_1+e_2a_2+\cdots+e_na_n$ 是 m^n 的倍数．其中，对于所有的 $i=1,2,\cdots,n$，$|e_i|<m$.

证明 设 B 是所有 $b=(b_1,b_2,\cdots,b_n)$ 构成的集合，其中所有 b_i 满足 $0\leqslant b_i<m$. 对于 $b\in B$，令

$$f(b)=b_1a_1+b_2a_2+\cdots+b_na_n.$$

若存在不同的 $b,b'\in B$，满足 $f(b)\equiv f(b')\pmod{m^n}$，则令 $e_i=b_i-b_i'$. 于是，有

$$e_1a_1+e_2a_2+\cdots+e_na_n\equiv 0\pmod{m^n}.$$

若所有的 $f(b)$ 均模 m^n 不同余，由于 $|B|=m^n$，则 $f(b)$ 模 m^n 的余数分别为 $0,1,2,\cdots,m^n-1$.

考虑多项式 $\sum\limits_{b\in B}x^{f(b)}$. 令 $x=e^{\frac{2\pi i}{m^n}}$，则

$$\sum_{b\in B}x^{f(b)}=1+x+x^2+\cdots+m^{m^n-1}=\frac{1-x^{m^n}}{1-x}=0.$$

另一方面

$$\sum_{b\in B}x^{f(b)}=\prod_{i=1}^{n}(1+x^{a_i}+x^{2a_i}+\cdots+x^{(m-1)a_i})=\prod_{i=1}^{n}\frac{1-x^{ma_i}}{1-x}.$$

由于 ma_i 不是 m^n 的倍数，所以，当 $x=e^{\frac{2\pi i}{m^n}}$ 时，$\sum\limits_{b\in B}x^{f(b)}\neq 0$. 矛盾.

例 11 （第 32 届俄罗斯数学奥林匹克题）证明：如果正整数 N 可以表示为都是 3 的倍数的三个整数的平方和，那么，它必可表示为都不是 3 的倍数的三个整数的平方和.

证明 由题意可知，正整数 N 可以表示为和式

$$9^n(a^2+b^2+c^2), \quad ①$$

其中，n 为正整数，a，b，c 为整数，a 不是 3 的倍数.

引理 所有形如和式①的正整数均可表示为 $9^{n-1}(x^2+y^2+z^2)$ 的形式，其中，x，y，z 为整数，且 x，y，z 都不是 3 的倍数.

引理的证明：不失一般性，可设 $a+b+c$ 不是 3 的倍数（否则，可将 a 换为 $-a$），有

$$\begin{aligned}9(a^2+b^2+c^2)&=(4a^2+4b^2+4c^2)+(a^2+4b^2+4c^2)+(4a^2+b^2+4c^2)\\&=(2a+2b-c)^2+(2b+2c-a)^2+(2a+2c-b)^2,\end{aligned}$$

其中，$2a+2b-c$，$2b+2c-a$，$2a+2c-b$ 都不是 3 的倍数，因为它们被 3 除的余数都与 $2(a+b+c)$ 相同，而后者不是 3 的倍数.

为完成对题中断言的证明，只需将这一引理使用 n 次.

例 12 （2003 年日本数学奥林匹克题）已知两个相异的正整数 a 和 b，且 b 为 a 的倍数．若用十进制表示，则 a 和 b 都由 $2n$ 组成，且最大有效位非零．又 a 的前 n 位和 b 的后 n 位相同，反之亦然，例如 $n=2$，$a=1234$，$b=3412$（但这个例子不满足 b 是 a 的倍数的条件），求 a 和 b．

解 用 2 个 n 位的正整数 x 和 y 表示 a 和 b，则

$a=10^nx+y$，$b=10^ny+x$．

由题设有 $x<y$，且 $10^ny+x=m(10^nx+y)$，其中 $2\leqslant m\leqslant 9$．

两边同时加 10^nx+y 得

$$(x+y)(10^n+1)=(m+1)(10^nx+y).\qquad ①$$

假设 $m+1$ 和 10^n+1 是互素的，则

$10^nx+y\equiv 0(\bmod (10^n+1))$．

所以，$x\equiv y(\bmod (10^n+1))$．

因为 x，y 只有 n 位，这与 $x<y$ 矛盾．

因为 $m+1\leqslant 10$，所以，$m+1$ 和 10^n+1 有一个共同的素因子，且必须是整数 2，3，5，7 之一．但 2，3，5 不能整除 10^n+1，故只能是 7．所以，

$m=6$，且 $7k=10^n+1$．

故式①变为

$(x+y)7k=7[(7k-1)x+y]$，即 $5kx=(k-1)(y-x)$．

注意到 $7(k-1)=10^n-6$，知 5 和 $k-1$ 互素．

于是，$5k$ 和 $k-1$ 也互素．

所以，$y-x$ 是 $5k$ 的整数倍．

因为 $0<y-x<10^n+1=7k$，则 $y-x=5k$．

所以，$x=k-1$，$y=6k-1$，且

$$a=10^nx+y=10^n(k-1)+(6k-1)$$
$$=10^n\left[\frac{1}{7}(10^n+1)-1\right]+\left[\frac{6}{7}(10^n+1)-1\right]=\frac{1}{7}(10^{2n}-1),$$

$$b=ma=\frac{6}{7}(10^{2n}-1).$$

其中，$n\equiv 3(\bmod 6)$（因为 10^n+1 是 7 的倍数）．

例 13 （CMO－18 试题）求所有满足 $a\geqslant 2$，$m\geqslant 2$ 的三元正整数组 (a,m,n)，使得 a^n+203 是 a^m+1 的倍数．

解 对于 n，m 分三种情况讨论．

(i) $n<m$ 时，由 $a^n+203\geqslant a^m+1$，有

$202\geqslant a^m-a^n\geqslant a^n(a-1)\geqslant a(a-1)$，

所以 $2\leqslant a\leqslant 14$.

当 $a=2$ 时，n 可取 1，2，…，7；

当 $a=3$ 时，n 可取 1，2，3，4；

当 $a=4$ 时，n 可取 1，2，3；

当 $5\leqslant a\leqslant 6$ 时，n 可取 1，2；

当 $7\leqslant a\leqslant 14$ 时，$n=1$.

由 $a^m+1\mid a^n+203$ 可知，解为(2,2,1)、(2,3,2)和(5,2,1).

(ii) $n=m$ 时，$a^m+1\mid 202$. 由于 202 仅有 1，2，101，202 共 4 个约数，而 $a\geqslant 2$，$m\geqslant 2$，$a^m+1\geqslant 5$，故 $a^m=100$ 或 201. 又 $m\geqslant 2$，所以解为(10，2，2).

(iii) $n>m$ 时，由 $a^m+1\mid 203(a^m+1)$，有

$a^m+1\mid a^n+203-(203a^m+203)$，即 $a^m+1\mid a^m(a^{n-m}-203)$.

又 $(a^m+1,a^m)=1$，所以

$a^m+1\mid a^{n-m}-203$.

①若 $a^{n-m}<203$，则令 $n-m=s\geqslant 1$，有 $a^m+1\mid 203-a^s$. 所以

$203-a^s\geqslant a^m+1$,

$202\geqslant a^s+a^m\geqslant a^m+a=a(a^{m-1}+1)\geqslant a(a+1)$,

$2\leqslant a\leqslant 13$.

类似于 (i) 的讨论，可知 (a,m,s) 的解为：

(2，2，3)，(2，6，3)，(2，4，4)，(2，3，5)，(2，2，7)，(3，2，1)，(4，2，2)，(5，2，3)，(8，2，1).

于是，(a,m,n) 为：

(2，2，5)，(2，6，9)，(2，4，8)，(2，3，8)，(2，2，9)，(3，2，3)，(4，2，4)，(5，2，5)，(8，2，3).

②$a^{n-m}=203$ 时，则 $a=203$，$n-m=1$，即解为

$(203,m,m+1)$，$m\geqslant 2$.

③$a^{n-m}>203$ 时，令 $n-m=s\geqslant 1$，则 $a^m+1\mid a^s-203$.

又 $a^s-203\geqslant a^m+1$，则 $s>m$. 由

$a^m+1\mid a^s+203a^m=(a^{s-m}+203)a^m=(a^{n-2m}+203)a^m$,

$(a^m+1,a^m)=1$,

所以 $a^m+1\mid a^{n-2m}+203$.

又 $s>m\Leftrightarrow n-m>m\Leftrightarrow n>2m\Leftrightarrow n-2m>0$. 此时的解只能由前面的解派生出来，即由 $(a,m,n)\to(a,m,n+2m)\to\cdots\to(a,m,n+2km)$，且每一个派生出的解都满足 $a^m+1\mid a^n+203$.

综上所述，所有解(a,m,n)为：

$(2,2,4k+1)$，$(2,3,6k+2)$，$(2,4,8k+8)$，$(2,6,12k+9)$，$(3,2,4k+3)$，

$(4,2,4k+4)$，$(5,2,4k+1)$，$(8,2,4k+3)$，$(10,2,4k+2)$，$(203,m,(2k+1)m+1)$，其中k为任意非负整数，且$m\geqslant 2$为整数.

2. 灵活应用约数的性质处理问题

例 14 （第 30 届俄罗斯数学奥林匹克题）3 个正整数中的任何两个数之积可以被该两数之和整除. 证明：这 3 个正整数具有大于 1 的公约数.

证明 将这 3 个正整数分别记为a，b，c，并记$x=(b,c)$，$y=(c,a)$，$z=(a,b)$. 假设a，b，c没有大于 1 的公约数，于是，x，y，z两两互素. 可设$a=kyz$，$b=lxz$，$c=mxy$，其中k，l，m为某些正整数.

由最大公约数的定义知k，l，m两两互素，并且ky也与lx互素. 但由题中条件$(kyz+lxz)\mid(kyz\cdot lxz)$知

$(kyz+lxz)\mid(ky\cdot lx\cdot z^2)$.

则$(ky+lx)\mid(ky\cdot lx\cdot z)$.

我们指出，$(ky,ky+lx)=(ky,lx)=1$.

同理，$(lx,ky+lx)=1$.

故$(ky+lx)\mid z$.

从而，$z\geqslant ky+lx\geqslant x+y$.

经过类似讨论，亦可得到$x\geqslant y+z$和$y\geqslant x+z$. 但是，这三个不等式不可能同时成立，矛盾.

例 15 （2005 年巴西数学奥林匹克题）给出正整数a，c和整数b. 证明：存在一个正整数x，满足$a^x+x\equiv b \pmod c$，即存在一个正整数x，使得c为数a^x+x-b的约数.

证明 设l是数列a，a^2，a^3，a^4，…，mod c的周期，则对任何正整数k和充分大的正整数i，有

$$a^{i+lk}\equiv a^i \pmod c. \qquad ①$$

设$d=\gcd(l,c)$表示l，c的最大公约数，则存在正整数u，v，满足$ul\equiv vd \pmod c$.

首先，断定如果$c>1$，那么，有$d<c$.

由$d=\gcd(l,c)$，所以，$d\leqslant c$.

反设$d=c$，由$c\mid l$，得$c\leqslant l$.

如果在一个模周期内余数两两不等，则$c\geqslant l$.

从而，$c=l$.

这说明存在正整数 n，使得 $c\mid a^{n}$，所以，

$c\mid a^{n+\omega}$ $(\omega\in\mathbf{N}_+)$. 因此，$l=c=1$.

所以，$c>1$ 意味着 $d<c$.

下面对 c 归纳证明.

当 $c=1$ 时，命题显然成立.

假设对于所有的正整数 $y(1\leqslant y<c)$命题都成立.

由于此时 $d<c$，利用归纳假设，取 $b=i(i=0,1,\cdots,d-1)$，存在一列充分大的整数列$\{n_0,n_1,\cdots,n_{d-1}\}$，使得 $a^{n_i}+n_i\equiv i(\bmod d)$.

设 $b=qd+r(0\leqslant r\leqslant d-1)$.

由 $a^{n_r}+n_r\equiv r+md(\bmod c)$和式①有.

$$a^{n_r+lk}+n_r+lk\equiv a^{n_r}+n_r+lk\equiv r+md+lk(\bmod c). \quad ②$$

但是当 k 改变时，$lk(\bmod c)$取遍 d 的所有倍数，于是，存在 k 使得

$$lk\equiv(q-m)d(\bmod c). \quad ③$$

把式③代入式②得

$$a^{n_r+lk}+n_r+lk\equiv r+md+(q-m)d=r+qd=b(\bmod c).$$

因此，取 $x=n_r+lk$ 完成归纳证明.

例 16 （2003 年女子数学奥林匹克题）对于任意正整数 n，记 n 的所有正约数组成的集合为 S_n. 证明：S_n 中至多有一半元素的个位数为 3.

证明 我们考虑如下三种情况：

(1) n 能被 5 整除，设 d_1，d_2，…，d_m 为 S_n 中所有个位数为 3 的元素，则 S_n 中还包括 $5d_1$，$5d_2$，…，$5d_m$ 这 m 个个位数为 5 的元素，所以 S_n 中至多有一半元素的个位数为 3.

(2) n 不能被 5 整除，且 n 的素因子的个位数均为 1 或 9，则 S_n 中所有的元素的个位数均为 1 或 9. 结论成立.

(3) n 不能被 5 整除，且 n 有个位数为 3 或 7 的素因子 p，令 $n=p^rq$，其中 q 和 r 都是正整数，p 和 q 互素. 设 $S_q=\{a_1, a_2, \cdots, a_k\}$ 为 q 的所有正约数组成的集合，将 S_n 中的元素写成如下方阵：

a_1，a_1p，a_1p^2，…，a_1p^r，

a_2，a_2p，a_2p^2，…，a_2p^r，

……

a_k，a_kp，a_kp^2，…，a_kp^r.

对于 $d_i=a_rp^l$，选择 a_rp^{l-1}或 a_rp^{l+1}之一与之配对（所选之数必须在 S_n 中）. 设 e_i 为所选之数，我们称(d_i,e_i)为一对朋友. 如果 d_i 的个位数为 3，则由 p 的个位数是

3 或 7，知 e_i 的个位数不是 3. 假设 d_i 和 d_j 的个位数都是 3，且有相同的朋友 $e=a_sp^t$，则 $\{d_i,d_j\}=\{a_sp^{t-1},a_sp^{t+1}\}$，因为 p 的个位数为 3 或 7，所以 p^2 的个位数是 9，而 n 不能被 5 整除，故 a_s 的个位数不为 0，所以 a_sp^{t-1}，$a_sp^{t-1}\cdot p^2=a_sp^{t+1}$ 的个位数不同，这与 d_i 和 d_j 的个位数都是 3 矛盾，所以，每个个位数为 3 的 d_i 均有不同的朋友.

综上所述，S_n 中每个个位数为 3 的元素，均与一个 S_n 中个位数不为 3 的元素为朋友，而且两个个位数为 3 的不同元素的朋友也是不同的，所以，S_n 中至多有一半元素的个位数为 3.

例 17 （2003 年国家队培训题）求所有的正整数 $n>1$，使得它的任何一个大于 1 的正约数具有 a^r+1 的形式，这里 a 为正整数，r 为大于 1 的正整数.

解 设 n 是符合条件的正整数，则 n 的每个大于 1 的约数都符合条件.

当 $n>2$ 时，我们可写 $n=a^r+1(r>1,a>1)$，使得其中的 a 取最小值，那么 r 为偶数. 因为若 r 为奇数，则 $a+1|n$，故存在正整数 b，$t(t>1)$，使得 $a+1=b^t+1$，得 $a=b^t$，$n=b^{tr}+1$，与 a 的最小性矛盾. 因此，n 等于一个完全平方数加上 1.

显然，形如 a^2+1 的素数都符合条件. 下面考虑 n 为合数的情形.

若 n 有两个奇素因子 p，q（p，q 可以相同），则 p，q 与 pq 都符合条件，即存在正整数 a，b，c，使得 $p=4a^2+1$，$q=4b^2+1$，$pq=4c^2+1$，于是

$$(4a^2+1)(4b^2+1)=4c^2+1. \quad ①$$

不妨设 $a\leqslant b$，则由①可知

$$4a^2(4b^2+1)=4(c-b)(c+b).$$

结合 $4b^2+1$ 为素数，可知 $4b^2+1|c-b$ 或者 $4b^2+1|c+b$，故 $c\geqslant 4b^2-b+1$. 利用 $a\leqslant b$，代入①式，易知①的右边比左边大. 矛盾.

又 4 不是一个符合条件的数，故合数 $n=2p$，p 为奇素数. 此时，存在正整数 a，b，使得

$$2(a^2+1)=b^2+1，即 a^2+1=(b-a)(b+a).$$

由于 a^2+1 为素数，所以，$(b-a,b+a)=(1,a^2+1)$，解得 $a=2$，$b=3$，故 $n=10$.

综上，符合条件的数为 10 或者形如 a^2+1 的素数.

综上可知 $\frac{r_1}{r}=\frac{r_2}{r}$，$r_1=r_2$.

3. 抓住最大公约数条件

例 18 （1985 年第 3 届美国数学邀请赛题）数列 101，104，116，…的通项是 $a_n=100+n^2$，其中 $n=1$，2，3，…. 对于每一个 n，用 d_n 表示 a_n 与 a_{n+1} 的最大公约数. 求 d_n 的最大值，其中 n 取一切正整数.

解 我们可以证明更一般的结论：

如果 a 是正整数，且 d_n 是 $a+n^2$ 与 $a+(n+1)^2$ 的最大公约数，则当 $n=2a$ 时，

d_n 达到最大值是 $4a+1$.

由于 d_n 是 $a+n^2$ 与 $a+(n+1)^2$ 的最大公约数，则

$d_n\mid(a+n^2)$，$d_n\mid[a+(n+1)^2]$.

从而 $d_n\mid[a+(n+1)^2]-(a+n^2)$，即

$d_n\mid(2n+1)$. ①

又因为 $2(a+n^2)=n(2n+1)+(2a-n)$，则由 $d_n\mid(a+n^2)$，$d_n\mid(2n+1)$ 得

$d_n\mid(2a-n)$. ②

由①，②知 $d_n\mid[(2n+1)+2(2a-n)]$，即 $d_n\mid(4a+1)$.

因此有 $1\leqslant d_n\leqslant 4a+1$.

下面我们证明 d_n 可以达到 $4a+1$.

事实上，当 $n=2a$ 时，

$a+n^2=a(4a+1)$，

$a+(n+1)^2=(a+1)(4a+1)$.

因为 $(a,a+1)=1$，所以

$a+n^2$ 和 $a+(n+1)^2$ 的最大公约数为 $4a+1$.

所以 d_n 达到的最大值为 $4a+1$.

特别地，当 $a=100$ 时，d_n 的最大值为 401.

例 19 （IMO－28 预选题）A 为整数组成的无限集，每一元素 $a\in A$ 是至多 1987 个素数的乘积（重数计算在内）．证明：必存在一个无限集 $B\subset A$ 及一个正整数 b，使 B 中任意两个数的最大公约数为 b.

证明 （1）若每个素数都只是集合 A 中有限多个元素的约数，那么可取一个 A 的子集 B，使 B 是无限集，且 B 中每两个数都互素（即 $b=1$）.

具体构造 B 的方法如下：

先取元素 a_1，再取与 a_1 互素的数 a_2，再取与 a_1，a_2 互素的数 a_3．由于 A 中每一元素都至多有 1987 个素约数，且每个素数都只是集合 A 中有限多个元素的约数，所以这样的取法是可以做到的.

一般地，当取定 a_1，a_2，…，a_{n-1} 之后，再取 a_n 与这 $n-1$ 个数互素.

这样得到的 $B=\{a_1, a_2, \cdots, a_{n-1}, a_n, \cdots\}$ 及 $b=1$ 符合题目的要求.

（2）若存在素数 p_1 为 A 中无限多个元素的约数，考虑集合

$$A_1=\left\{\frac{a}{p_1}，p_1\mid a，a\in A\right\}，$$

则 A_1 是无限集.

这时有两种可能：

或者存在无限集 $B_1\subset A_1$，B_1 中每两个数都互素，从而取集合 B，使 B 中的元

素由 B_1 中的每个元素的 p_1 倍组成，则 B 及 $b-p_1$ 符合题目要求.

或者存在无限集

$$A_2=\left\{\frac{a}{p_1p_2},\ p_1p_2 \mid a,\ a\in A\right\}.$$

如此继续下去，由于 A 中每个元素至多有 1987 个素约数，所以最终将得到符合要求的无限集 B 及数 b.

例 20 （IMO－29 预选题）斐波那契数定义为

$a_0=0,\ a_1=a_2=1,\ a_{n+1}=a_n+a_{n-1}\ (n\geqslant1).$

求第 1960 项与 1988 项的最大公约数.

解 由 $a_1=a_2=1$ 及

$$a_{n+1}=a_n+a_{n-1}\ (n>1) \quad ①$$

可逐步算出数列的前 28 项为：

1，1，2，3，5，8，13，21，34，55，89，144，233，377，610，987，1597，2584，4181，6765，10946，17711，28657，46368，75025，121393，196418，317811.

对斐波那契数，我们证明

$$(a_m,a_n)=a_{(m,n)}. \quad ②$$

首先用数学归纳法证明

$$(a_n,a_{n-1})=1. \quad ③$$

当 $n=1$ 时，$(a_1,a_0)=1$，

当 $n=2$ 时，$(a_2,a_1)=(1,1)=1$.

所以当 $n=1$，2 时，③式成立.

假设当 $n=k$ 时，③式成立，即 $(a_k,a_{k-1})=1$.

则由①式 $(a_{k+1},a_k)=(a_k,a_{k-1})=1$.

所以对所有自然数 n，③式成立.

我们设 $m\geqslant n$，由①式可推出

$$a_m=a_na_{m-n+1}+a_{n-1}a_{m-n}. \quad ④$$

由④可以看出，a_{m-n} 与 a_n 的最大公约数一定是 a_m 的约数，a_m 与 a_n 的最大公约数一定是 $a_{n-1}a_{m-n}$ 的约数.

由③，a_n 与 a_{n-1} 互素，则 a_m 与 a_n 的最大公约数也是 a_{m-n} 的约数，所以

$$(a_m,a_n)=(a_{m-n},a_n). \quad ⑤$$

设 $m=qn+r$，$0\leqslant r<n$，则由⑤得 $(a_m,a_n)=(a_r,a_n)$.

注意到 $(m,n)=(r,n)$.

由 $n>r$，继续上面的过程可得 $(a_m,a_n)=a_{(m,n)}$.

由于$(1988,1960)=28$,则

$(a_{1988},a_{1960})=a_{(1988,1960)}=a_{28}=317811.$

例21 (IMO-31预选题)数列$\{u_n\}$定义为

$u_1=1,u_2=1,u_n=u_{n-1}+2u_{n-2},n=3,4,\cdots.$

证明对任意自然数$n,p(p>1)$有$u_{n+p}=u_{n+1}u_p+2u_nu_{p-1}$.求出$u_n$与$u_{n+3}$的最大公约数.

证明 $u_{n+p}=u_{n+p-1}+2u_{n+p-2}$,

$u_{n+p-1}=u_{n+p-2}+2u_{n+p-3}$,

……

$u_{n+2}=u_{n+1}+2u_n$.

将以上各式分别乘以u_1,u_2,…,u_{p-1},得

$u_1u_{n+p}=u_1u_{n+p-1}+2u_1u_{n+p-2}$,

$u_2u_{n+p-1}=u_2u_{n+p-2}+2u_2u_{n+p-3}$,

……

$u_{p-1}u_{n+2}=u_{p-1}u_{n+1}+2u_{p-1}u_n$.

相加得

$$\begin{aligned}u_{n+p}&=u_{n+p-1}(u_1-u_2)+u_{n+p-2}(u_1+2u_1-u_3)+\cdots+u_{n+1}(u_{p-1}+2u_{p-2})+2u_{p-1}u_n\\&=u_{n+1}u_p+2u_{p-1}u_n.\end{aligned}$$

在上式中取$p=3$得

$u_{n+3}=u_{n+1}u_3+2u_nu_2=3u_{n+1}+2u_n$.

从而u_{n+3}与u_n的最大公约数为

$(u_{n+3},u_n)=d\mid 3u_{n+1}$.

由$u_1=1,u_2=1$是奇数,及$u_n=u_{n-1}+2u_{n-2}$可推出u_n均为奇数,从而由$u_n=u_{n-1}+2u_{n-2}$可知

$(u_n,u_{n-1})=(u_{n-1},u_{n-2})=\cdots=(u_2,u_1)=1$.

于是由$d\mid u_n,d\mid 3u_{n+1}$得$d\mid 3$,即$d=1$或3.

再由$u_{n+3}=u_{n+2}+2u_{n+1},u_{n+2}=u_{n+1}+2u_n$,相加可得

$u_{n+3}=3u_{n+1}+2u_n$.

由此易得,当且仅当$3\mid n$时,$3\mid u_n$.

所以有$d=(u_n,u_{n+3})=\begin{cases}1,若3\nmid n;\\3,若3\mid n.\end{cases}$

例22 (IMO-26预选题)设$S_n=\sum\limits_{k=1}^{n}(k^5+k^7)$,求$S_n$与$S_{3n}$的最大公约数.

解 由于 $S_1=1^5+1^7=2$,

$S_2=(1^5+1^7)+(2^5+2^7)=2\cdot 81=2\cdot(1+2)^4$,

$S_3=2\cdot 3^4+(3^5+3^7)=2\cdot 6^4=2\cdot(1+2+3)^4$,

$S_4=2\cdot 6^4+(4^5+4^7)=2^5\cdot 5^4=2\cdot(1+2+3+4)^4$.

由此猜想,

$$S_n=2(1+2+\cdots+n)^4. \quad ①$$

下面用数学归纳法证明.

$n=1$ 时,显然成立.

假设 $n=k$ 时,①式成立,那么 $n=k+1$ 时,

$$\begin{aligned}S_{k+1}&=2(1+2+\cdots+k)^4+(k+1)^5+(k+1)^7\\&=\frac{1}{8}k^4(k+1)^4+(k+1)^5+(k+1)^7\\&=\frac{1}{8}(k+1)^4[k^4+8(k+1)+8(k+1)^3]\\&=\frac{1}{8}(k+1)^4(k^4+8k^3+24k^2+32k+16)\\&=\frac{1}{8}(k+1)^4(k+2)^4\\&=2[1+2+\cdots+k+(k+1)]^4.\end{aligned}$$

所以 $n=k+1$ 时,①式成立.

于是对所有自然数 n,①式成立.

因此 $S_n=2\cdot\left[\dfrac{n(n+1)}{2}\right]^4, S_{3n}=2\cdot\left[\dfrac{3n(3n+1)}{2}\right]^4$.

(1) 当 $n=2k$ 时,

$$\begin{aligned}d&=(S_n,S_{3n})=\left(2\cdot\left[\frac{2k(2k+1)}{2}\right]^4,2\cdot\left[\frac{6k(6k+1)}{2}\right]^4\right)\\&=(2k^4(2k+1)^4,2\cdot 81k^4(6k+1)^4).\end{aligned}$$

因为 $(2k+1,6k+1)=1$,所以 $d=2k^4((2k+1)^4,81)$.

当 $k=3t+1$ 时,

$(2k+1)^4=(6t+3)^4=81(2t+1)^4$.

所以 $d=2\cdot 81k^4=2\cdot 81\cdot\dfrac{n^4}{2^4}=\dfrac{81}{8}n^4$.

当 $k\neq 3t+1$ 时,$d=2k^4=\dfrac{n^4}{8}$.

(2) 当 $n=2k+1$ 时,

$S_n=2[(2k+1)(k+1)]^4, S_{3n}=2[3(2k+1)(3k+2)]^4$.

因为$(3k+2,2k+1)=1,(3k+2,k+1)=1$,所以

$d=2(2k+1)^4(3^4,(k+1)^4)$.

当 $k=3t+2$ 时,$k+1=3(t+1)$,所以

$d=2n^4\cdot 3^4=162n^4$.

当 $k\neq 3t+2$ 时,$d=2n^4$.

例 23 (1988 年第 22 届全苏数学奥林匹克题)数列$\{a_n\}$由如下关系式定义:

$a_0=0, a_n=P(a_{n-1}), n=1,2,\cdots$,

其中 $P(x)$为某个正整数系数的多项式.

证明对于任何两个具有最大公约数 d 的自然数 m 和 k,数 a_m 和 a_k 的最大公约数都是 a_d.

证法 1 先证明如下的引理:

如果整数数列 $a_0=0$,a_1,a_2,a_3,…具有性质:

对任何下标 $m>k\geqslant 1$,都有

$$(a_m,a_k)=(a_{m-k},a_k), \quad ①$$

则必有$(a_m,a_k)=a_d$.

其中 $d=(m,k)$,记号(x,y)表示 x 和 y 的最大公约数.

事实上,由$(m,k)=(m-k,k)$,我们可从任何数对(m,k)开始,反复运用$(m,k)\to(m-k,k)$,即由数对中的较大者减去其中的较小者,而保持较小者不动,终将得到数对$(d,0)$,其中 $d=(m,k)$.实际上,这正是通常的辗转相除法.

这样,由①式即可推得

$(a_m,a_k)=(a_{m-k},a_k)=\cdots=(a_d,a_0)=a_d$.

下面再来证明问题本身.

记 $\underbrace{P(P(P\cdots(P}_{n\text{重}}(x))\cdots))=P_n(x)$,则 $P_n(x)$为整系数多项式,且有

$a_m=P_m(a_0)$及 $a_m=P_{m-k}(a_k), m>k$.

若记 $P_n(x)=a_n+xQ_n(x)$,则 $Q_n(x)$也是整系数多项式.

下面只需再验证①式成立即可.

对 $m>k\geqslant 1$,我们有

$(a_m,a_k)=(P_{m-k}(a_k),a_k)=(a_{m-k}+a_kQ_{m-k}(a_k),a_k)=(a_{m-k},a_k)$.

因而①式成立.

由引理,即有$(a_m,a_k)=a_d$,其中 $d=(m,k)$.

证法 2 我们用数学归纳法证明:

对一切自然数 $m\leqslant n$ 和 $k\leqslant n$,有

$(a_m, a_k)=a_d$, ①

其中 $d=(m,k)$.

当 $n=1$ 时,结论显然成立.

假设对一切 $n\leqslant n_0$ 结论成立,我们证明当 $n=n_0+1$ 时结论也成立.

如果 $m\leqslant n_0$,且 $k\leqslant n_0$,那么由归纳假设可知,等式①成立.

如果 $m=k=n_0+1$,①显然成立.

剩下只要考察 m 或者 k,其中一个等于 n_0+1,而另一个不超过 n_0 的情形.

为确定起见,设 $m=n_0+1$,$k\leqslant n_0$.

那么 $n_0=m-1\geqslant m-k=n_0-k+1\geqslant 1$,即 $m-k$ 是不超过 n_0 的自然数.

因此,由于 $(m,k)=(m-k,k)$ 及归纳假设,有

$a_d=a_{(m,k)}=a_{(m-k,k)}=(a_{m-k}, a_k)$. ②

所以为了证明当 $m=n_0+1$,$k\leqslant n_0$ 时,等式①成立,只要验证

$(a_m, a_k)=(a_{m-k}, a_k)$.

由已知条件得 $a_m=P_{m-k}(a_k)$,其中记号 $P_n(x)$ 同证法 1. 又记

$P_n(x)=a_n+xQ_n(x)$,

则同证法 1,有

$(a_m, a_k)=(a_{m-k}, a_k)$.

于是由②式有 $(a_m, a_k)=a_d$.

因而①式对 $m=n_0+1$, $k\leqslant n_0$ 成立.

从而对所有 $m\leqslant n$, $k\leqslant n$, ①式成立.

例 24 (IMO-18 试题)求出同时满足如下条件的集合 S 的元素个数的最大值:

(1) S 中的每个元素都是不超过 100 的正整数;

(2) 对于 S 中任何两个不同的元素 a, b, 都存在 S 中的元素 c, 使得 a 与 c 的最大公约数等于 1, 并且 b 与 c 的最大公约数也等于 1;

(3) 对于 S 中任意两个不同的元素 a, b, 都存在 S 中异于 a, b 的元素 d, 使得 a 与 d 的最大公约数大于 1, 并且 b 与 d 的最大公约数也大于 1.

解 最大个数为 72.

将不超过 100 的每个正整数 n 表示成

$n=2^{\alpha_1}\cdot 3^{\alpha_2}\cdot 5^{\alpha_3}\cdot 7^{\alpha_4}\cdot 11^{\alpha_5}\cdot q$,

其中 q 是不能被 2, 3, 5, 7, 11 整除的正整数, α_1, α_2, α_3, α_4, α_5 为非负整数.

我们选取满足条件"α_1, α_2, α_3, α_4, α_5 中恰有 1 个或 2 个非零"的那些正整数组成集合 S, 即 S 中包括 50 个偶数 2, 4, …, 98, 100, 但除去 $2\times3\times5$, $2^2\times3\times5$, $2\times3^2\times5$, $2\times3\times7$, $2^2\times3\times7$, $2\times5\times7$, $2\times3\times11$ 这 7 个数; 3 的奇数倍 $3\times$

1，3×3，…，3×33 共 17 个数；最小素因子为 5 的数 5×1，5×5，5×7，5×11，5×13，5×17，5×19 共 7 个数；最小素因子为 7 的数 7×1，7×7，7×11，7×13 共 4 个数；以及素数 11. 从而，S 中总共有$(50-7)+17+7+4+1=72$ 个数.

下面证明如此构造的 S 满足题述条件.

条件（1）显然满足.

对于条件（2），注意到在$[a,b]$的素因子中至多出现 2，3，5，7，11 中的 4 个数，记某个未出现的数为 p，显然 $p\in S$，并且

$(p,a)\leqslant(p,[a,b])=1,(p,b)\leqslant(p,[a,b])=1.$

于是，取 $c=p$ 即可.

对于条件（3），当$(a,b)=1$ 时，取 a 的最小素因子 p 和 b 的最小素因子 q，易见 $p\neq q$，并且 p、$q\in\{2,3,5,7,11\}$. 于是，$pq\in S$，并且

$(pq,a)\geqslant p>1,(pq,b)\geqslant q>1.$

a,b 互素保证了 pq 异于 a,b. 从而，取 $d=pq$ 即可.

当$(a,b)=e>1$ 时，取 p 为 e 的最小素因子，q 为满足 $q\nmid[a,b]$的最小素数，易见 $p\neq q$，并且 $p,q\in\{2,3,5,7,11\}$. 于是，$pq\in S$，并且

$(pq,a)\geqslant(p,a)=p>1,(pq,b)\geqslant(p,b)=p>1.$

$q\nmid[a,b]$ 保证了 pq 异于 a，b. 从而，取 $d=pq$ 即可.

下面证明任意满足题述条件的集合 S 的元素数目不会超过 72.

显然，$1\notin S$. 对于任意两个大于 10 的素数 p，q，因为与 p，q 均不互素的数最小是 pq，已大于 100，故据条件（3）知，10 与 100 之间的 21 个素数 11，13，…，89，97 中最多有一个出现在 S 中. 记除 1 和这 21 个素数外的其余 78 个不超过 100 的自然数构成集合 T，我们断言 T 中至少有 7 个数不在 S 中，从而 S 中最多有 $78-7+1=72$ 个元素.

(i) 当有某个大于 10 的素数 p 属于 S 时，S 中所有各数最小素因子只可能是 2，3，5，7 和 p. 运用条件（2）可得出以下结论：

①若 $7p\in S$，因 $2\times3\times5$，$2^2\times3\times5$，$2\times3^2\times5$ 与 $7p$ 包括了所有的最小素因子，故由条件（2）知，$2\times3\times5$，$2^2\times3\times5$，$2\times3^2\times5\notin S$；若 $7p\notin S$，注意 $2\times7p>100$，而 $p\in S$，故由条件（3）知 7×1，7×7，7×11，$7\times13\notin S$.

②若 $5p\in S$，则 $2\times3\times7$，$2^2\times3\times7\notin S$；若 $5p\notin S$，则 5×1，$5\times5\notin S$.

③$2\times5\times7$ 与 $3p$ 不同属于 S.

④$2\times3p$ 与 5×7 不同属于 S.

⑤若 $5p$，$7p\notin S$，则 $5\times7\notin S$.

当 $p=11$ 或 13 时，由①，②，③，④可分别得出至少有 3，2，1，1 个 T 中的

数不属于S，合计7个；当$p=17$或19时，由①，②，③可分别得出至少有4，2，1个T中的数不属于S，合计7个；当$p>20$时，由①，②，③分别有至少4，2，1个T中的数不属于S，合计也是7个.

(ii) 如果没有大于10的素数属于S，则S中的最小素因子只可能是2，3，5，7. 于是，下面7对数中的每对都不能同时在S中出现：

$(3,2\times5\times7),(5,2\times3\times7),(7,2\times3\times5),(2\times3,5\times7),(2\times5,3\times7),(2\times7,3\times5),(2^2\times7,3^2\times5)$.

从而，T中至少有7个数不在S中.

综上所述，本题的答案为72.

4. 关注最小公倍数性质

例25 （1987年第5届美国数学邀请赛题）设$[r,s]$表示正整数r和s的最小公倍数. 求有序三元正整数组(a,b,c)的个数，其中$[a,b]=1000,[b,c]=2000,[c,a]=2000$.

解 由$[a,b]=1000,[b,c]=2000,[c,a]=2000$可知：$a,b,c$均为$2^m\cdot5^n$型的数.

不妨设$a=2^{m_1}5^{n_1},b=2^{m_2}5^{n_2},c=2^{m_3}5^{n_3}$.

由$[a,b]=2^3\cdot5^3,[b,c]=[c,a]=2^4\cdot5^3$及最小公倍数的性质可得

$\max\{m_1,m_2\}=3,\max\{m_2,m_3\}=4,\max\{m_3,m_1\}=4$,

$\max\{n_1,n_2\}=3,\max\{n_2,n_3\}=3,\max\{n_3,n_1\}=3$.

由此可知，$m_3=4$，m_1和m_2中必有一个是3，此时另一个可取0，1，2或3，不计重复，一共有7种不同情况.

n_1，n_2，n_3中必有两个数是3，此时第3个数可取0，1，2或3，不计重复，一共有10种不同情况.

从而满足本题条件的数组(a,b,c)共有$7\cdot10=70$（个）.

例26 （1991年澳大利亚数学竞赛题）M_n为1，2，…，n的最小公倍数（如$M_1=1$，$M_2=2$，$M_3=6$，$M_4=12$，$M_5=60$，$M_6=60$）. 对什么样的正整数n，$M_{n-1}=M_n$成立. 证明你的结论.

解 若n是某个素数的幂，即$n=p^k$，p是素数，则

$M_n=[1,2,\cdots,n-1,n]=[M_{n-1},n]=[M_{n-1},p^k]=pM_{n-1}$.

此时 $M_{n-1}\neq M_n$.

若n不是某个素数的幂. 设$n=ab,1<a<n,1<b<n$,则

$a\leqslant n-1,b\leqslant n-1$.

再令$(a,b)=1$,则$a\mid M_{n-1}$，$b\mid M_{n-1}$.

所以 $n=ab\mid M_{n-1}$.

于是 $M_n=M_{n-1}$.

因此，$M_{n-1}=M_n$ 的充要条件是：自然数 n 不是某个素数的幂.

例 27 （1997 年加拿大数学奥林匹克题）有多少对正整数 x，y 满足条件 $(x,y)=5!$ 且 $[x,y]=50!$.

解 设 7 到 47 之间的素数 7，11，13，17，19，23，29，31，37，41，43，47 依次用 p_1，p_2，…，p_{12} 表示，则

$5!=2^3\cdot3^1\cdot5^1\cdot p_1^0\cdot p_2^0\cdot\cdots\cdot p_{12}^0$，

$50!=2^{a_1}\cdot3^{a_2}\cdot5^{a_3}\cdot p_1^{b_1}\cdot p_2^{b_2}\cdot\cdots\cdot p_{12}^{b_{12}}$.

由于 $x\mid50!$，$y\mid50!$，所以 x，y 具有下面的形式：

$x=2^{n_1}\cdot3^{n_2}\cdot5^{n_3}\cdot p_1^{n_4}\cdot\cdots\cdot p_{12}^{n_{15}}$，

$y=2^{m_1}\cdot3^{m_2}\cdot5^{m_3}\cdot p_1^{m_4}\cdot\cdots\cdot p_{12}^{m_{15}}$.

其中 $\max\{n_i,m_i\}$ 是 50! 的第 i 个素数的指数，$\min\{n_i,m_i\}$ 是 5! 的第 i 个素数的指数.

在不考虑 $x<y$ 的情况下，$n_i(i=1,2,\cdots,15)$ 的选取方式有两种，所以 x 的个数为 2^{15} 个.

当 x 选定之后，y 是唯一确定的.

又当 x 取定之后，得到 y，有 $x<y$ 或 $x>y$ 两种可能.

故满足题设条件的正整数对有 $\frac{2^{15}}{2}=2^{14}$ 个.

例 28 （1992 年加拿大数学奥林匹克训练题）若 $n,a_1,a_2,\cdots,a_k$ 是整数，$n\geqslant a_1>a_2>\cdots>a_k>0$，且对于所有的 i 与 j，a_i 和 a_j 的最小公倍数不超过 n. 证明对于 $1\leqslant i\leqslant k$，$ia_i\leqslant n$.

证明 我们对 i 用数学归纳法.

(1) 当 $i=1$ 时，由题设 $a_1\leqslant n$，所以 $i=1$ 时结论正确.

(2) 假设结论对小于或等于 $i-1$ 的正整数都成立.

若对于某些整数 p 和 q，

$[a_{i-1},a_i]=pa_{i-1}=qa_i$.

因为 $a_{i-1}>a_i$，则 $q>p$.

如果 $q<i$，则

$i(q-p)\geqslant i>q$，即 $(i-1)q>ip$，$\frac{p}{q}<\frac{i-1}{i}$.

由归纳假设可推出

$ia_i=ia_{i-1}\cdot\frac{p}{q}<ia_{i-1}\cdot\frac{i-1}{i}=(i-1)a_{i-1}\leqslant n$.

如果 $q\geqslant i$，则由归纳假设有

$ia_i\leqslant qa_i=[a_{i-1},a_i]\leqslant n$.

于是结论对 i 成立.

由 (1), (2),对所有的 $1\leqslant i\leqslant k, ia_i\leqslant n$ 成立.

例 29 (1990 年国家集训队培训题)设 $a_1,a_2,\cdots,a_n$ 为正整数,均不超过 $2n$, $n\neq 4$. 证明 $\min\limits_{1\leqslant i<j\leqslant n}[a_i,a_j]\leqslant 6\left(\left[\frac{n}{2}\right]+1\right)$. 记号 $[a_i,a_j]$ 表示 a_i 和 a_j 的最小公倍数.

证明 (1) 若 $a_1,a_2,\cdots,a_n$ 中有一个是另一个的倍数,则

$$\min_{1\leqslant i<j\leqslant n}[a_i,a_j]\leqslant 2n\leqslant 6\left(\left[\frac{n}{2}\right]+1\right)$$

成立.

(2) 若 $a_1,a_2,\cdots,a_n$ 中每一个均不是其他数的倍数.

若 $a_i\leqslant n$,则用 $2a_i$ 代替 a_i,于是总可以假定

$\{a_1,a_2,\cdots,a_n\}=\{n+1,n+2,\cdots,2n\}=A$.

(i) 若 $2\mid n+1$,则 $\frac{3}{2}(n+1)\in A$.

$$\min_{1\leqslant i<j\leqslant n}[a_i,a_j]\leqslant\left[n+1,\frac{3}{2}(n+1)\right]=3(n+1)=6\left(\left[\frac{n}{2}\right]+1\right).$$

(ii) 若 $2\mid n+2$.

当 $n>4$ 时, $\frac{3}{2}(n+2)\in A$.

$$\min_{1\leqslant i<j\leqslant n}[a_i,a_j]\leqslant\left[n+2,\frac{3}{2}(n+2)\right]=3(n+2)=6\left(\left[\frac{n}{2}\right]+1\right).$$

当 $n=2$ 时, $A=\{3,4\}$,则

$$[3,4]=12=6\left(\left[\frac{2}{2}\right]+1\right).$$

由以上,命题得证.

例 30 (1994 年第 20 届全俄数学奥林匹克题)求证对于正整数 k,m 和 n,有

$[k,m]\cdot[m,n]\cdot[n,k]\geqslant[k,m,n]^2$.

这里 $[a,b,\cdots,z]$ 表示正整数 $a,b,\cdots,z$ 的最小公倍数.

证明 设 k,m,n 的素因子标准分解式为

$$k=\prod_{i=1}^{t}p_i^{\alpha_i},m=\prod_{i=1}^{t}p_i^{\beta_i},n=\prod_{i=1}^{t}p_i^{\gamma_i}.$$

这里 $p_i(i=1,2,\cdots,t)$ 为素数, $\alpha_i,\beta_i,\gamma_i(i=1,2,\cdots,t)$ 为非负整数. 则

$$[k,m]=\prod_{i=1}^{t}p_i^{\max(\alpha_i,\beta_i)},[m,n]=\prod_{i=1}^{t}p_i^{\max(\beta_i,\gamma_i)},[n,k]=\prod_{i=1}^{t}p_i^{\max(\gamma_i,\alpha_i)},$$

$$[k,m,n]=\prod_{i=1}^{t}p_i^{\max(\alpha_i,\beta_i,\gamma_i)},[k,m,n]^2=\prod_{i=1}^{t}p_i^{2\max(\alpha_i,\beta_i,\gamma_i)}.$$

将 $\alpha_i,\beta_i,\gamma_i(1\leqslant i\leqslant t)$ 中最小的一个记为 α_i^*，最大的一个记为 γ_i^*，中间一个记为 β_i^*，即有 $\alpha_i^*\leqslant\beta_i^*\leqslant\gamma_i^*$.

于是有

$$\max(\alpha_i,\beta_i)+\max(\beta_i,\gamma_i)+\max(\gamma_i,\alpha_i)=\beta_i^*+\gamma_i^*+\gamma_i^*=\beta_i^*+2\gamma_i^*$$
$$\geqslant 2\gamma_i^*=2\max(\alpha_i,\beta_i,\gamma_i).$$

这样就有

$$[k,m]\cdot[m,n]\cdot[n,k]=\prod_{i=1}^{t}p_i^{\max(\alpha_i,\beta_i)+\max(\beta_i,\gamma_i)+\max(\gamma_i,\alpha_i)}$$
$$\geqslant\prod_{i=1}^{t}p_i^{2\max(\alpha_i,\beta_i,\gamma_i)}=[k,m,n]^2.$$

【模拟实战】

1. 100 个正整数之和为 101101，则它们的最大公约数的最大可能值是多少？证明你的结论.
2. 两数之和为 667，它们的最小公倍数除以最大公约数所得的商等于 120，求这两数.
3. （第 48 届斯洛文尼亚数学奥林匹克题）马休先按顺序写出了 1 到 10000 的全部数字，然后擦去了那些既不能被 5 整除，又不能被 11 整除的数，在剩下的数中，位于第 2004 位的数是多少？
4. （第 32 届俄罗斯数学奥林匹克题）正整数 N 不能被 81 整除，但是可以表示为都是 3 的倍数的三个整数的平方和. 证明：它也可以表示为都不是 3 的倍数的三个整数的平方和.
5. （IMO－29 预选题）若 r 是 1059，1417 与 2312 被 d 除后的余数，这里 d 是大于 1 的整数，求 $d-r$ 的值.
6. （2006 年法国国家队选拔考试题）设 $A_1,A_2,\cdots,A_n$ 是 n 个等差数列，每个等差数列由 k 项组成，且任两个等差数列至少有 2 个公共元素. 若这些等差数列中有 b 个的公差为 d_1，而其他的等差数列的公差为 d_2，其中 $0<b<n$. 证明：

   $$b\leqslant 2\left(k-\frac{d_2}{\gcd(d_1,d_2)}\right)-1.$$
7. （2003 年白俄罗斯数学奥林匹克题）（1）若正整数 $k(k\geqslant3)$ 满足：有 k 个正整数，使得任意两个不互素，任意三个互素. 求 k 的所有可能值.

   （2）是否存在一个无穷项的正整数集，满足（1）的条件？
8. （IMO－45 预选题）一个从正整数集 $\mathbf{N}_+$ 到其自身的函数 f 满足：对于任意的 $m,n\in\mathbf{N}_+$，$(m^2+n)^2$ 可以被 $f^2(m)+f(n)$ 整除. 证明：对于每个 $n\in\mathbf{N}_+$，有 $f(n)=n$.

第十章　裴蜀定理

【基础知识】

裴蜀定理　设 a,b,d 是整数,则 $(a,b)=d$ 的充要条件是 $d|a,d|b$,存在整数 u,v,使得 $ua+vb=d$.

推论 1　$(a,b)=1$ 的充要条件是,存在整数 v,v,使得 $ua+vb=1$.

从而,当 $(a,b)=1$ 时,$ua+vb$ 可表示所有整数.由此,又得到下面的推论.

推论 2　a,b 均为正整数时,$(a,b)=1$ 的充要条件是,存在正整数 u,v,使得 $ua-vb=1$.

裴蜀定理还可以推广至多个数的最大公约数:

对于任意的正整数 $a_1,a_2,\cdots,a_n$,存在整数 $k_1,k_2,\cdots,k_n$,使得

$k_1a_1+k_2a_2+\cdots+k_na_n=(a_1,a_2,\cdots,a_n)$.

【典型例题与基本方法】

例 1　(第 1 届国际数学奥林匹克题)(1) 已知整数 a,b,c,d 满足 $ad-bc=1$.求证:$\frac{a+b}{c+d}$是既约分数(即 $a+b$ 与 $c+d$ 互素).

(2) 证明对任意自然数 n,分数$\frac{21n+4}{14n+3}$不可约(即为既约分数).

证明　(1) 由于 $a(c+d)-c(a+b)=ad-bc=1$,这说明 $c+d$ 与 $a+b$ 互素,即$\frac{a+b}{c+d}$是既约分数.

(2) 注意到 $(14n+3)-2(7n+1)=1$,由裴蜀定理,知 $14n+3$ 与 $7n+1$ 互素,即 $(7n+1,14n+3)=1$.

$(21n+4,14n+3)=(7n+1,14n+3)=1$.故$\frac{21n+4}{14n+3}$不可约.

例 2　(2000 年普特南数学竞赛题)设 $n\geqslant m\geqslant 1$,n,m 为整数.证明:$\frac{(m,n)}{n}\cdot C_n^m$为整数.

证明　本题的关键是如何表示 (m,n).

由裴蜀定理知，存在 $r,t\in\mathbf{Z}$，使得 $mr+nt=(m,n)$. 故

$$\frac{(m,n)}{n}\cdot C_n^m=\frac{mr+nt}{n}\cdot C_n^m=r\cdot\frac{m}{n}\cdot C_n^m+tC_n^m=rC_{n-1}^{m-1}+tC_n^m\in\mathbf{Z}.$$

例 3 已知一个角的度数为 $\frac{180^\circ}{n}$，其中 n 是不被 3 整除的正整数. 证明这个角可以用圆规与直尺三等分.

证明 因为 n 与 3 互素，由裴蜀定理，有

$$1=un-3v,$$

其中，u,v 均为正整数. 从而

$$\frac{60^\circ}{n}=u\cdot 60^\circ-\frac{180^\circ}{n}\cdot v.$$

这表明先作角等于 $u\cdot 60^\circ$（60° 角可用圆规和直尺作出），然后再减去 $v\cdot\frac{180^\circ}{n}$ $\left(\frac{180^\circ}{n}\text{是已知角}\right)$，就产生 $\frac{60^\circ}{n}$ 的角，即 $\frac{180^\circ}{n}$ 的 $\frac{1}{3}$.

注 并不是每一个角都能用尺规三等分的，例如 60° 的角就无法用尺规三等分，此时 $n=3$.

例 4 证明：存在一个有理数 $\frac{c}{d}$，其中 $d<100$，能使 $\left[k\cdot\frac{c}{d}\right]=\left[k\cdot\frac{73}{100}\right]$，对于 $k=1,2,\cdots,99$ 均成立. 这里 $[x]$ 表示实数的整数部分，即不超过 x 的最大整数（可参见本书第十五章）.

证明 首先注意到 73 与 100 互素，因此有 c,d 存在，使 $73d-100c=1$.

下证对于任一 $k\in\{1,2,\cdots,99\}$，题设结论成立.

事实上，可设 $\left[\frac{kc}{d}\right]=n$，由于 $k<100$，

$$\frac{73}{100}k-\frac{kc}{d}=\frac{k(73d-100c)}{100d}=\frac{k}{100d},$$

所以，$0<\frac{73k}{100}-\frac{kc}{d}<\frac{1}{d}$.

注意到 $\left[\frac{kc}{d}\right]=n$，则 $\frac{kc}{d}<n+1=\frac{(n+1)}{d}d$.

所以 $\frac{73k}{100}<\frac{kc+1}{d}\leqslant\frac{(n+1)d}{d}=n+1$.

从而 $\left[\frac{73k}{100}\right]=n=\left[\frac{kc}{d}\right]$.

【解题思维策略分析】

1. 适时运用裴蜀定理

例 5 （1965 年第 5 届全俄数学奥林匹克题）给定两个互素的自然数 p 和 q. 整数 n 如果能表示成 $n=px+qy$ 的形式，其中 x、y 为非负整数，则称 n 是“好的”，在相反的情况下，则称 n 是“坏的”.

（1）证明存在整数 c，使整数 n 与 $c-n$ 中始终一个是好的，一个是坏的.

（2）坏的非负整数共有多少个.

解 （1）如果 p,q 是互素的自然数，那么每一个整数 z 都能表示为 $z=px+qy$ 的形式.

并且若 $x=a,y=b$ 满足上式，则有 $z=p(a-qt)+q(b+pt)(t\in\mathbf{Z})$.

同时，对于 $0\leqslant x\leqslant q-1$，存在唯一的表达式.

我们可以把每一个整数 z 与整数对 (x,y) 相对应. 这里 $0\leqslant x\leqslant q-1,z=px+qy$. 同时不同的数与不同的数对相对应，而且仅当 $y\geqslant 0$ 时，z 是好的.

如果数 $z=px+qy(0\leqslant x\leqslant q-1)$ 是好数，那么 $z'=(q-1-x)p+(-1-y)q$ 就是坏数，反过来，如果 z 是坏数，则 z' 是好数. 而且点 (x,y) 和点 $(q-1-x,-1-y)$ 关于点 $(x_0,y_0)=\left(\frac{q-1}{2},-\frac{1}{2}\right)$ 对称，而数 z 和 z' 关于点 $z_0=px_0+qy_0=\frac{pq-p-q}{2}$ 对称，因为 $z+z'=pq-p-q=2z_0=c$.

所以，好数 z 对应于坏数 $z'=c-z$，反过来也对.

（2）因为最小的好数是 0，那么最大的坏数将是 c，所以共有 $\frac{c+1}{2}=\frac{(p-1)(q-1)}{2}$ 个坏数.

例 6 （2008 年全国高中数学联赛题）设 $f(x)$ 是周期函数，T 和 1 是 $f(x)$ 的周期且 $0<T<1$. 证明：

（1）若 T 为有理数，则存在素数 p，使 $\frac{1}{p}$ 是 $f(x)$ 的周期；

（2）若 T 为无理数，则存在各项均为无理数的数列 $\{a_n\}$ 满足 $1>a_n>a_{n+1}>0(n=1,2,\cdots)$，且每个 $a_n(n=1,2,\cdots)$ 都是 $f(x)$ 的周期.

证明 （1）若 T 是有理数，则存在正整数 m,n，使得 $T=\frac{n}{m}$ 且 $(m,n)=1$. 从而，由裴蜀定理知，存在整数 a,b，使得 $ma+nb=1$. 于是，

$\frac{1}{m}=\frac{ma+nb}{m}=a+bT=a\times 1+bT$ 是 $f(x)$ 的周期.

又因 $0<T<1$，所以，$m\geqslant 2$.

设 p 是 m 的素因子，则

$m=pm'(m'\in\mathbf{N}_+)$.

从而，$\frac{1}{p}=m'\cdot\frac{1}{m}$ 是 $f(x)$ 的周期.

(2) 若 T 是无理数，令 $a_1=1-\left[\frac{1}{T}\right]T$，其中，$[x]$ 表示不超过实数 x 的最大整数，则 $0<a_1<1$，且 a_1 是无理数.

令 $a_2=1-\left[\frac{1}{a_1}\right]a_1,\cdots,a_{n+1}=1-\left[\frac{1}{a_n}\right]a_n,\cdots$

由数学归纳法易知，a_n 均为无理数且 $0<a_n<1$.

又 $\frac{1}{a_n}-\left[\frac{1}{a_n}\right]<1$，故 $1<a_n+\left[\frac{1}{a_n}\right]a_n$，即 $a_{n+1}=1-\left[\frac{1}{a_n}\right]a_n<a_n$.

因此，$\{a_n\}$ 是递减数列.

接下来证明：每个 a_n 是 $f(x)$ 的周期.

事实上，因 1 和 T 是 $f(x)$ 的周期，所以 $a_1=1-\left[\frac{1}{T}\right]T$ 亦是 $f(x)$ 的周期. 假设 a_k 是 $f(x)$ 的周期，则 $a_{k+1}=1-\left[\frac{1}{a_k}\right]a_k$ 也是 $f(x)$ 的周期.

由数学归纳法，已证得 a_n 均是 $f(x)$ 的周期.

例 7 (2005 年德国数学奥林匹克题)在平面上的每个整点 (x,y) (x,y 都是整数)处放一盏灯，当时刻 $t=0$ 时，仅有一盏灯亮着；当 $t=1,2,\cdots$ 时，满足下列条件的灯被打开：至少与一盏亮着的灯的距离为 2005. 证明：所有的灯都能被打开.

证明 设最初亮灯为 O，对某点 A，$\boldsymbol{OA}=(x,y)$.

$2005^2=1357^2+1476^2$.

$(1357,1476)=(1357,119)=(1357,7\times17)=1$.

令 $\boldsymbol{a}=(1357,1476)$，$\boldsymbol{b}=(1476,1357)$，$\boldsymbol{c}=(1357,-1476)$，$\boldsymbol{d}=(1476,-1357)$.

若在 t 时刻 A 被点亮，则在下一时刻 $A+\boldsymbol{a}$，$A+\boldsymbol{b}$，$A+\boldsymbol{c}$，$A+\boldsymbol{d}$ 分别被点亮.

只须证对任意的 A，存在 $p,q,r,s\in\mathbf{Z}$，使

$$\boldsymbol{OA}=p\boldsymbol{a}+q\boldsymbol{b}+r\boldsymbol{c}+s\boldsymbol{d}. \quad ①$$

因为 $(1357,1476)=1$，由裴蜀定理知，存在 $m_0,n_0,u_0,v_0\in\mathbf{Z}$，满足

$x=1357m_0+1476n_0$，$y=1357u_0+1476v_0$.

令 $m=m_0+1476k$，$n=n_0-1357k$，$u=u_0+1476l$，$v=v_0-1357l(k,l\in\mathbf{Z})$.

$$2\mid(m-v)\Leftrightarrow2\mid(m_0-v_0+1476k+1357l)\Leftrightarrow2\mid(m_0-v_0+l), \quad ②$$

$$2\mid(u-n)\Leftrightarrow2\mid(u_0-n_0+1476l+1357k)\Leftrightarrow2\mid(u_0-n_0+k). \quad ③$$

显然存在 $k,l\in\mathbf{Z}$ 满足式②，③.

令$\begin{cases}p+r=m,\\p-r=v,\end{cases}\begin{cases}q+s=n,\\q-s=u,\end{cases}$则

$$\begin{cases}p=\dfrac{m+v}{2},\\r=\dfrac{m-v}{2},\end{cases}\begin{cases}q=\dfrac{n+u}{2},\\s=\dfrac{n-u}{2}.\end{cases}$$

显然，$p,q,r,s\in\mathbf{Z}$满足式①.

所以，总可经过有限次操作使A被点亮.

例 8 （2007年国家队培训题）是否存在正整数a,b满足a不整除b^n-n对所有的正整数n成立？

证明 不存在.

下面证明，对于任意的正整数a,b均存在正整数n使得$a\mid b^n-n$.

我们对a归纳：

(1) 当$a=1$时显然成立.

(2) 假设小于a时成立，当为a时，

(i) 存在素数p满足$p\mid(a,b)$时，设$a=p^la_0$，$p\nmid a_0$，取$k>l$使$a_0\mid p^k-1$，再取$b_0=b^{p^k}$. 由归纳假设知，存在正整数n_0使得$a_0\mid b_0^{n_0}-n_0$. 这样

$0\equiv b_0^{n_0}-n_0\equiv b^{p^kn_0}-n_0\equiv b^{p^kn_0}-n_0-(p^k-1)n_0\equiv b^{p^kn_0}-p^kn_0\pmod{a_0}$.

记$n=p^kn_0$，则$a_0\mid b^n-n$. 又$l<k<n$，$p\mid b$，故$p^l\mid b^n$，$p^l\mid n$，这样$p^l\mid b^n-n$.

所以$a\mid b^n-n$.

(ii) 不存在素数p满足$p\mid(a,b)$，即$(a,b)=1$时，则$b^{\varphi(a)}\equiv1\pmod a$.

设$d=(a,\varphi(a))$，则$d<a$，由归纳假设知，存在正整数n_0使得$d\mid b^{n_0}-n_0$. 故对于任意正整数k_0使得$d\mid b^{n_0+k_0\varphi(a)}-[n_0+k_0\varphi(a)]$.

由裴蜀定理知，存在正整数x,y使得$x\varphi(x)-ya=d$. 取

$k_0=kx$，$b^{n_0+k_0\varphi(a)}\equiv b^{n_0}\pmod a$.

而$n_0+k_0\cdot\varphi(a)=n_0+kx\cdot\varphi(a)\equiv n_0+kd\pmod a$，故

当k取遍$\bmod\dfrac{a}{d}$的一个完系时，$b^{n_0+k_0\varphi(a)}-[n_0+k_0\varphi(a)]$取遍$\bmod a$意义下被$d$整除的那部分剩余系. 特别地，存在正整数$k$使得

$a\mid b^{n_0+k_0\varphi(a)}-[n_0+k_0\varphi(a)]$，

此时取$n=n_0+kx\cdot\varphi(a)$即符合题意.

由 (i) (ii) 可知当其为a时也成立.

由数学归纳法可知，对于任意的正整数a,b均存在正整数n使得$a\mid b^n-n$，即不存在正整数a,b满足a不整除b^n-n对所有的正整数n成立.

2. 进行转化运用裴蜀定理

例 9 (1988 年国家集训队选拔考试题)设 $f(x)=3x+2$,证明:存在正整数 m,使得 $f^{(100)}(m)$ 能被 1988 整除,其中 $f^{(k)}(x)$ 表示 $\underbrace{f(f(\cdots f}_{k\text{个}f}(x)\cdots))$.

证明 先由不动点知识求出 $f^{(100)}(m)$ 的表达式,再由题设数字特征分析出 $(3^n,1988)=1$(n 为自然数).

由题设知,迭代不动点为 $x=-1$,再由数学归纳法知 $f^{(100)}(n)=3^{100}(n+1)-1$,则 $f^{(100)}(m)=3^{100}(m+1)-1=3^{100}m+3^{100}-1$.

因为 $(3^{100},1988)=1$,由裴蜀定理推论 2 可知,存在自然数 u,v,使得 $1988u-3^{100}v=1$,则 $1988\mid(1+3^{100}v)$,从而,

$1988\mid[(3^{100}-1)(1+3^{100}v)]$.

令 $m=(3^{100}-1)v$,则 $1988\mid f^{100}(m)$.

例 10 (IMO-26 试题)设 n,k 为正整数,$(k,n)=1$,且 $0<k<n$,再设 $M=\{1,2,\cdots,n-1\}$.现对集合 M 中的每个 i 涂上蓝色或白色,且满足:

(a) i 和 $n-i$ 要同色;

(b) 当 $i\neq k$ 时,i 和 $|k-i|$ 要同色.

求证:所有的数都同色.

证明 由 $(k,n)=1$,借助裴蜀定理分类可证所有的 $i\in M$ 与 k 同色.讨论过程中要注意由 (b) 可得两个结论:一是 M 中 k 的整数倍与 k 同色;二是 $i>k$ 时,i 与 $i-qk$ 同色($i-qk>0$).

据题设可知存在整数 x,y 使得 $i=xk+yn$.由 $1\leqslant i\leqslant n-1$ 可知,x,y 的取值无外乎以下三种情形:

(1) $x>0,y=0$; (2) $x>0,y<0$; (3) $x<0,y>0$.

(1) 时结论成立,而 (3) 可化为 (2) 讨论.因为由(a)可知,i 和 $n-i=(-x)k+(-y+1)n$ 同色.若 $-y+1=0$,则化为 (1).若 $-y+1<0$,就化为 (2).综上可知只须讨论 (2).

对于 (2) (必有 $x>-y$),这时又分为三类:(i) $k=i$;(ii) $k>i$;(iii) $k<i$.对于 (i),由 (1) 显然成立.当 (iii) 出现时,由带余除法可知,$i=qk+i'$,$0\leqslant i'<k$,($q,i\in\mathbf{Z}$).

若 $i'=0$,则由 (1) 结论成立.若 $1\leqslant i'<k$,由条件 (b) 可知,i 和 $i'=i-qk=(x-q)\cdot k+yn$ 同色,用 i' 代替 i 讨论就化为 (ii).

当 (ii) 出现时,由条件 (b) 可知,i 和 $k-i=(-x+1)k-yn$ 同色;再由条件 (a) 可知,i 和 $i''=n-(k-i)=(x-1)k+(y+1)n$ 同色.若 $y+1=0$,则结论成立.若 $y+1<0$,又化为情形 (2).继续对 i'' 分 (i),(ii),(iii) 三种情况考虑,这样经过有限

次讨论后(因为 $y<0$,且每讨论一次 y 增加1,这样若干次后变为0),总可得到 i 和 $x'k$ 同色,即 i 和 k 同色.

例 11 (2004年美国数学奥林匹克题)设 $a_1,a_2,\cdots,a_n$ 是整数,它们的最大公约数等于1.设 S 是具有下述性质的一个由整数组成的集合:

(1) $a_i\in S,i=1,2,\cdots,n$;

(2) $a_i-a_j\in S,1\leqslant i,j\leqslant n(i,j$ 可以相同);

(3) 对任意整数 $x,y\in S$,若 $x+y\in S$,则 $x-y\in S$.

证明:S 等于由所有整数组成的集合.

证明 将命题加强:我们证明对任意 $t\in\mathbf{Z}$,数 $(a_1,a_2,\cdots,a_n)t\in S$,这里 $(a_1,a_2,\cdots,a_n)$ 表示 $a_1,\cdots,a_n$ 的最大公约数,在 $n=1$ 时,$(a_1)=a_1$. ①

对 n 归纳予以处理.当 $n=1$ 时,先证对任意 $t\in\mathbf{N}^*$,均有 $a_1t\in S$.事实上,在条件(2)中令 $i=j=1$,就有 $0\in S$,结合 $a_1\in S$ 及条件(3)可知 $-a_1\in S$;现在设 $-a_1,0,a_1,2a_1,\cdots,(t-1)a_1$ 都属于 $S(t\in\mathbf{N}^*)$,则由 $(t-1)a_1\in S,-a_1\in S$ 及 $(t-2)a_1\in S$,利用条件(3)可知 $(t-1)a_1-(-a_1)=ta_1\in S$.所以,对任意 $t\in\mathbf{N}^*$,数 $ta_1\in S$.进一步,由 $0\in S,ta_1\in S$ 知 $0-ta_1\in S$,即 $-ta_1\in S$.所以,对任意 $t\in\mathbf{Z}$,均有 $ta_1\in S$,命题①对 $n=1$ 成立.

当 $n=2$ 时,由前已证:对任意 $x,y\in\mathbf{Z}$,均有 $xa_1\in S,ya_2\in S$.下证:对任意 $k_1,k_2\in\mathbf{Z}$,均有 $k_1a_1+k_2a_2\in S$. ②

为此对 $k=|k_1|+|k_2|$ 予以归纳.当 $k=0$ 时,$k_1=k_2=0$,命题②显然成立;当 $k=1$ 时,由 $\pm a_1\in S,\pm a_2\in S$ 知②成立;当 $k=2$ 时,由条件(2)知 $a_1-a_2\in S$,结合 $a_1,-a_2\in S$ 及条件(3)可知 $a_1-(-a_2)=a_1+a_2\in S$,再由 $0,a_1+a_2\in S$ 知 $0-(a_1+a_2)=-a_1-a_2\in S$,结合 $-2a_1\in S,-2a_2\in S$ 可知②成立.现在设②对 $0,1,2,\cdots,k-1$ 都成立,考虑 $k(\geqslant3)$ 的情形.这时,$|k_1|+|k_2|\geqslant3$,故 $|k_1|$ 与 $|k_2|$ 中必有一个不小于2,不妨设 $|k_1|\geqslant2$.若 $k_1\geqslant2$,由归纳假设知 $(k_1-1)a_1+k_2a_2\in S,(k_1-2)a_1+k_2a_2\in S$,结合 $-a_1\in S$ 及条件(3)知 $(k_1-1)a_1+k_2a_2-(-a_1)=k_1a_1+k_2a_2\in S$,若 $k_1\leqslant-2$,由归纳假设知 $(k_1+1)a_1+k_2a_2\in S,(k_2+2)a_1+k_2a_2\in S$,结合 $a_1\in S$ 及条件(3)知 $(k_1+1)a_1+k_2a_2-a_1=k_1a_1+k_2a_2\in S$.从而命题②对 k 成立.这表明命题②是正确的.

由命题②及裴蜀定理,知对任意 $t\in\mathbf{Z}$,均有 $(a_1,a_2)t\in S$,即命题①对 $n=2$ 成立.

现在我们设命题①对 $1,2,\cdots,n-1$ 都成立,考虑 $n(\geqslant3)$ 的情形.此时,记 $(a_1,a_2,\cdots,a_n)=d,(a_2,a_3,\cdots,a_n)=d_1,(a_1,a_3,\cdots,a_n)=d_2,(a_1,a_2,a_4,\cdots,a_n)=d_3$.由归纳假设可知,对任意 $t_1,t_2,t_3\in\mathbf{Z}$,都有 $d_1t_1\in S,d_2t_2\in S,d_3t_3\in S$.

由 d 及 d_1,d_2,d_3 的定义知 $d=(d_1,d_2)=(d_1,d_3)=(d_2,d_3)$.设 $d_i=x_id,i=1,2,3$,则 x_1,x_2,x_3 两两互素,故 x_1,x_2,x_3 中必有一个为奇数,不妨设 x_3 为奇数.下证:对

任意 $t\in\mathbf{Z}$,存在 $m_1,m_2,m_3\in\mathbf{Z}$,使得

$$d_1m_1+d_2m_2=d_3m_3 \text{ 且 } d_1m_1-d_2m_2=dt. \quad ③$$

事实上,对任意 $t\in\mathbf{Z}$,由 $(x_1,x_2)=1$,可知存在 $y\in\mathbf{Z}$,使得 $x_1y\equiv t(\mathrm{mod}\ x_2)$,于是,令 $l=2x_1y-t$,就有 $l+t\equiv0(\mathrm{mod}\ 2x_1)$,$l-t\equiv0(\mathrm{mod}\ 2x_2)$. 而由 x_3 为奇数,及 x_1,x_2,x_3 两两互素,可知 $(x_3,2x_1x_2)=1$,于是存在 $m_3\in\mathbf{Z}$ 使得 $m_3x_3\equiv l(\mathrm{mod}\ 2x_1x_2)$. 因此,令 $m=\frac{m_3x_3+t}{2x_1}$,$m_2=\frac{m_3x_3-t}{2x_2}$,则 $m_1,m_2\in\mathbf{Z}$,且 m_1,m_2,m_3 满足③.

由归纳假设及③中的结论,知 $d_1m_1\in S$,$d_2m_2\in S$,$d_1m_1+d_2m_2=d_3m_3\in S$,从而结合条件 (3),知 $dt=d_1m_1-d_2m_2\in S$. 所以,命题①对 n 成立.

综上可知,对任意 $t\in\mathbf{Z}$,数 $(a_1,a_2,\cdots,a_n)t\in S$,这样,由题给条件 $(a_1,\cdots,a_n)=1$,故每个整数 t 都属于 S,命题获证.

【模拟实战】

1. (1989 年全国高中数学联赛题)集合 $M=\{u|u=12m+8n+4l,m,n,l\in\mathbf{Z}\}$ 与 $N=\{u|u=20p+16q+12r,p,q,r\in\mathbf{Z}\}$ 的关系为(　　)

   A. $M=N$　　B. $M\not\subseteq N,N\not\subseteq M$　　C. $M\subset N$　　D. $M\supset N$

2. (2000 年全国高中数学联赛题)平面上整点(纵、横坐标都是整数的点)到直线 $y=\frac{5}{3}x+\frac{4}{5}$ 的距离中的最小值是(　　)

   A. $\frac{\sqrt{34}}{170}$　　B. $\frac{\sqrt{34}}{85}$　　C. $\frac{1}{20}$　　D. $\frac{1}{30}$

3. $\mathbf{C}$ 是复数集,设集合 $A=\{z|z^{18}=1,z\in\mathbf{C}\}$,$B=\{w|w^{48}=1,w\in\mathbf{C}\}$,$D=\{zw|z\in A,w\in B\}$. 求 D 的元素个数.

4. 数列 $f_{n+1}(x)=f_1(f_n(x))$,其中 $f_1(x)=2x+1$,$n\in\mathbf{N}$. 试证:对任意的 $n\in\{11,12,13,\cdots\}$,必存在一个由 n 唯一确定的 $m_0\in\{0,1,\cdots,1993\}$,使得 $1995|f_n(m_0)$.

5. 给定正整数 a,b,c,定义函数 $f(x,y,z)=ax+by+cz$,其中 $x,y,z\in\mathbf{Z}$. 试求 $f(x,y,z)$ 的最小正整数值.

6. 若 p,q 互素,且 $p,q\in\mathbf{N}$,则存在最小的 $m=pq-p-q+1$,使得对所有 $n\geqslant m$,n 都可写成 $n=px+qy$(x,y 是非负整数).

7. (胡生森老师根据第 26 届 IMO 预选题改编)m 个盒子中各放若干个球,每次在其中 $n(n<m)$ 个盒中各加一球,证明:当 $(m,n)=1$ 时,不论开始的分布情况如何,总可按上述方法进行有限次加球后,使得各盒子中的球数相等.

8. (IMO-40 试题)确定所有的正整数对 (n,p),满足:p 是一个素数,$n\leqslant2p$,且 $(p-1)^n+1$ 能够被 n^{p-1} 整除.

第十一章　互素数与欧拉函数

【基础知识】

1. 互素数

(1) 若$(a_1,a_2,\cdots,a_n)=1$,就叫做$a_1,a_2,\cdots,a_n$互素(也叫做互质),这n个数叫互素数(互质数).

特别地,1和任何整数互素;相邻两个整数互素;相邻两个奇数互素;对素数p,若p不能整除a,则p与a互素.

(2) 若$(a,b)=1$,则$(a\pm b,a)=1$,$(a\pm b,ab)=1$.

(3) 若$(a,b)=1$,$a|bc$,则$a|c$.

(4) 若$a|c$,$b|c$,$(a,b)=1$,则$ab|c$.

(5) 若$(a,b)=1$,则$(b,ac)=(b,c)$.

(6) 若$(a,b)=1$,$c|a$,则$(c,b)=1$.

(7) 若$(a,b)=1$,则$(a,b^k)=1$.

(8) 若$a_1,a_2,\cdots,a_m$中的每一个与$b_1,b_2,\cdots,b_n$中的每一个互素,则$(a_1a_2\cdots a_m,b_1b_2\cdots b_n)=1$.

2. 欧拉函数

小于m且与m互素的正整数的个数叫做欧拉函数,记作$\varphi(m)$.

若$m=\prod\limits_{i=1}^{n}p_i^{a_i}$,则$\varphi(m)=m\prod\limits_{i=1}^{n}\left(1-\dfrac{1}{p_i}\right)$.其中$p_i$是素数,$a_i$是正整数,$(i=1,2,\cdots,n)$.

当m为素数时,$\varphi(m)=m-1$.

当m为素数,k为正整数时,$\varphi(m^k)=m^{k-1}(m-1)$.

若$(a,b)=1$,则$\varphi(a,b)=\varphi(a)\cdot\varphi(b)$.

【典型例题与基本方法】

例1　(1987年第21届全苏数学奥林匹克题)求出这样一组五个不同的自然数,使得其中任意两个数互素,且任意若干个数(多于1个)之和为合数.

解　我们考虑一般的情形:

设 $a_1,a_2,\cdots,a_n$ 这 n 个数满足 $a_i=i\cdot n!+1,i=1,2,\cdots,n$.

则这 n 个数中任意两个数都互素.

否则,若 $(a_i,a_j)=d>1$,则由

$$a_i=i\cdot n!+1=pd, \qquad ①$$

$$a_j=j\cdot n!+1=qd, \qquad ②$$

得 $(i-j)n!=(p-q)d$.

于是 $d\mid(i-j)n!$

由①可知,d 不是 $2,3,\cdots,n$ 的约数,又由于 $|i-j|<n$,于是只有 $d=1$,即 a_i 与 a_j 互素.

此外,$a_1,a_2,\cdots,a_n$ 中任意 k 个数之和一定能被 k 整除.

因此,$a_i=i\cdot n!+1,i=1,2,\cdots,n$ 是满足题设条件的 n 个数.

特别地,$n=5$ 时,这五个数为 121,241,361,481,601.

例 2 (第 22 届伊朗数学奥林匹克题)设 $a_1,a_2,\cdots,a_n(n>1)$ 是不全相等的自然数. 证明:有无穷多个素数 p,对于每个 p,存在 $k\in\mathbf{N}_+$,满足 $p\mid(a_1^k+a_2^k+\cdots+a_n^k)$.

证明 可以假设 $a_1,a_2,\cdots,a_n$ 是互素的. 要不然,令 $d=(a_1,a_2,\cdots,a_n),a_i'=\frac{a_i}{d}$.

如果 $p\mid(a_1'^k a_2'^k+\cdots+a_n'^k)$,就可以得到 $p\mid(a_1^k+a_2^k+\cdots+a_n^k)$.

若结论不成立,设 $\{p_1,p_2,\cdots,p_s\}$ 是 $\{a_1^k+a_2^k+\cdots+a_n^k\mid k\in\mathbf{N}_+\}$ 的所有素数因子集合,存在一个数 t,满足 $p_i^t\nmid j,j=1,2,\cdots,n$.

令 $u=\varphi((p_1p_2\cdots p_s)^t)$.

数 a 满足 $b=au>t$.

考虑数 $c=a_1^b+a_2^b+\cdots+a_n^b$,$q$ 取 p_i 中的一个.

若 a_i 能被 q 整除,因为 $b>t$,就得到 $a_i^b\equiv0(\bmod q^t)$.

若 a_i 不能被 q 整除,就得到 $a_i^b\equiv1(\bmod q^t)$.

所以,c 模 q^t 的余数就是 $0,1,\cdots,n$ 中的其中一个.

因为不是所有的 a_i 都能被 q 整除,所以 $q^t\nmid c$. 故对于所选定的 t,c 都不能被 q^t 整除. 所以,

$$c\leqslant(p_1p_2\cdots p_s)^t.$$

可以找一个足够大的 b 使得 c 变得足够大(a_i 不全是 1),矛盾.

例 3 (IMO-45 预选题)设 k 是一个大于 1 的固定的整数,$m=4k^2-5$. 证明:存在正整数 a,b,使得如下定义的数列 $\{x_n\}$:

$$x_0=a,x_1=b,x_{n+2}=x_{n+1}+x_n,n=0,1,\cdots$$

其所有的项均与 m 互素.

证明 取 $a=1, b=2k^2+k-2$.

因为 $4k^2\equiv5 \pmod m$,所以,

$2b=4k^2+2k-4\equiv2k+1 \pmod m$,

$4b^2\equiv4k^2+4k+1\equiv4k+6\equiv4b+4 \pmod m$.

又因为 m 是奇数,所以,$b^2\equiv b+1 \pmod m$.

由于 $(b,m)=(2k^2+k-2,4k^2-5)=(2k^2+k-2,2k+1)=(2,2k+1)=1$,所以 $(b^n,m)=1$,其中 n 为任意正整数.

下面用数学归纳法证明.

当 $n\geqslant0$ 时,有 $x_n\equiv b^n \pmod m$.

当 $n=0,1$ 时,显然结论成立.

假设对于小于 n 的非负整数结论也成立,其中 $n\geqslant2$,则有

$x_n=x_{n-1}+x_{n-2}\equiv b^{n-1}+b^{n-2}\equiv b^{n-2}(b+1)\equiv b^{n-2}\cdot b^2\equiv b^n \pmod m$.

因此,对于所有的非负整数 n,有 $(x_n,m)=(b^n,m)=1$.

例 4 怎么样的正整数 x 满足 $\varphi(2x)=\varphi(3x)$.

解 设 $x=2^a3^by$,其中 a,b 为非负整数,$6\nmid y$.

若 $b>0$,则

$\varphi(2x)=\varphi(2^{a+1})\cdot\varphi(3^b)\cdot\varphi(y)=2^a\cdot3^{b-1}\cdot2\varphi(y)$,

$\varphi(3x)=\varphi(2^a)\cdot\varphi(3^{b+1})\cdot\varphi(y)=2^{a-1}\cdot3^b\cdot2\varphi(y)$.

因而 $\varphi(2x)\neq\varphi(3x)$. 所以,在 $\varphi(2x)=\varphi(3x)$ 时,$b=0, x=2^ay$.

这时,$\varphi(2x)=2^a\cdot\varphi(y)$,$\varphi(3x)=2\varphi(2^a)\cdot\varphi(y)$.

因而 $\varphi(2^a)=2^{a-1}$,$a>0$.

故 $x=2^ay$,a 为正整数,$6\nmid y$.

例 5 证明:$\varphi(n)=\frac{1}{4}n$ 不可能成立.

证明 若 $\varphi(n)=\frac{1}{4}n$,则 $4\mid n$.

设 $n=2^\alpha p_1^{\alpha_1}\cdots p_k^{\alpha_k}$,$p_i$ 为奇素数,$\alpha\geqslant2$,则

$2^{\alpha-2}p_1^{\alpha_1}\cdots p_k^{\alpha_k}=2^{\alpha-1}p_1^{\alpha_1-1}\cdots p_k^{\alpha_k-1}(p_1-1)\cdots(p_k-1)$,

于是 $p_1p_2\cdots p_k=2(p_1-1)\cdots(p_k-1)$.

上式右边为偶数,左边为奇数,矛盾!

故不存在 n,使得 $\varphi(n)=\frac{1}{4}n$.

例 6 设 $\tau(n)$ 表示正整数 n 的因数个数,求证:$\varphi(n)\cdot\tau(n)\geqslant n$.

证明 设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$,$\alpha_i$ 为非负整数.

注意到$\tau(n)=(a_1+1)(a_2+1)\cdots(a_s+1)\geqslant 2^s$，

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)$$
$$\geqslant n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2}\right)\cdots\left(1-\frac{1}{2}\right)=\frac{n}{2^s},$$

于是，$\varphi(n)\cdot\tau(n)\geqslant\frac{n}{2^s}\cdot 2^s=n$.

例 7 若$(m,n)=2$，则$\varphi(mn)=2\varphi(m)\cdot\varphi(n)$.

证明 设$m=2^a k$，$n=2l$，这里$a\geqslant 1$，且$(2,k)=1$，$(2,l)=1$，$(k,l)=1$. 于是，

$$\varphi(mn)=\varphi(2^{a+1}kl)=\varphi(2^{a+1})\varphi(k)\varphi(l)$$
$$=2^a\varphi(k)\varphi(l)=2\cdot[2^{a-1}\varphi(k)\cdot\varphi(l)]$$
$$=2\cdot\varphi(m)\cdot\varphi(n).$$

【解题思维策略分析】

1. 灵活运用互素数的性质

例 8 （第 30 届俄罗斯数学奥林匹克题）方程$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n=0$的系数$a_1,a_2,\cdots,a_{n-1},a_n$皆为非零整数. 证明：如果该方程有$n$个整数根，且它们两两互素，则$a_{n-1}$与$a_n$互素.

证明 假设a_{n-1}与a_n不互素，于是，它们有公共的素约数p，亦即$a_{n-1}=pm$，$a_n=pk$，其中m,k为整数. 设方程的n个整数根为$x_1,x_2,\cdots,x_n$.

由$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n=(x-x_1)(x-x_2)\cdots(x-x_n)$得

$$x_1x_2\cdots x_n=\pm a_n=\pm pk.$$

上式表明$x_1,x_2,\cdots,x_n$均非零，而且由该式和题意知$x_1,x_2,\cdots,x_n$中恰有 1 个是p的倍数，不妨设其为x_1. 由韦达定理知

$$\sum_{j=1}^{n}\frac{x_1x_2\cdots x_n}{x_j}=\pm a_{n-1}=\pm pm.$$

上式左端除了第一项$x_2x_3\cdots x_n$之外，其余各项都是x_1的倍数，因此，都是p的倍数；而右端是p的倍数，因此，$x_2x_3\cdots x_n$也是p的倍数，即$x_2,x_3,\cdots,x_n$中有 1 个是p的倍数. 故该数就与x_1有公共的质约数p，从而不互素，此与题意相矛盾.

所以，a_{n-1}与a_n互素.

例 9 （2005 年国家集训队测试题）求所有的正整数组(a,m,n)，满足：$a>1$，$m<n$，且a^m-1的素因子集合与a^n-1的素因子集合相同.

解 记$S(n)$为正整数n的不同素因子构成的集合. 先证明一个引理.

引理 若正整数$b>1$，p为素数，且$S(b^p-1)=S(b-1)$，则$p=2$，$b+1$是 2 的方幂.

引理的证明：假设 p 为奇素数，由于

$b^{p-1}+b^{p-2}+\cdots+b+1=(b^{p-1}-1)+\cdots+(b-1)+p.$

若 $p\nmid b-1$，则 $(b^{p-1}+b^{p-2}+\cdots+b+1,b-1)=(p,b-1)=1$，从而

$S(b^{p-1}+\cdots+b+1)\not\subseteq S(b-1)$，矛盾！

若 $p\mid b-1$，设 $b-1=p^s\cdot t,s,t\in\mathbf{Z}^+,p\nmid t$，则

$$b^p-1=(1+p^s\cdot t)^p-1=p\cdot p^s\cdot t+C_p^2\cdot(p^s\cdot t)^2+\cdots$$
$$=p^{s+1}\cdot t(1+p^s\cdot t\cdot x),x\in\mathbf{Z}^+.$$

因为 $(1+p^s\cdot t\cdot x,b-1)=(1+p^s\cdot t\cdot s,p^s\cdot t)=1$，所以 $S(b^p-1)\not\subseteq S(b-1)$，矛盾！

所以，$p=2,b^2-1=(b-1)(b+1)$.

若 b 为偶数，则 $(b-1,b+1)=1$，故 $S(b+1)\not\subseteq S(b-1)$，矛盾！

所以 b 为奇数，$b^2-1=4\cdot\dfrac{b-1}{2}\cdot\dfrac{b+1}{2}$.

因为 $\left(\dfrac{b-1}{2},\dfrac{b+1}{2}\right)=1$，故 $\dfrac{b+1}{2}$ 没有奇素因子[否则 $S(b+1)\not\subseteq S(b-1)$，矛盾]，即 $b+1$ 是 2 的方幂.

回到原题：设 $(m,n)=d$，可设 $n=kd$，由 $m<n$ 知 $k>1$. 熟知

$(a^m-1,a^n-1)=a^{(m,n)}-1=a^d-1$，

于是我们有

$S(a^m-1)=S(a^n-1)=S((a^m-1,a^n-1))=S(a^d-1)$.

令 $b=a^d$，则 $b>1$，且 $S(b-1)=S(b^k-1)$.

任取 k 的素因子 p，则

$b-1\mid b^p-1,b^p-1\mid b^k-1$，

故 $S(b^p-1)=S(b-1)$.

由引理知，$p=2,a^d+1=b+1$ 是 2 的方幂. 由 p 的任意性知 $k=2^r,r\in\mathbf{Z}^+$.

若 $r\geqslant2$，则 $S(b-1)=S(b^2-1)=S(b^4-1)=S(b^{2^r}-1)$.

仍由引理知，b^2+1 是 2 的方幂，但 $b^2+1\equiv2\pmod 4$，$b^2+1>2$. 矛盾！

所以，$r=1,k=2$.

设 $a^d+1=2^l,l\in\mathbf{Z}^+,l\geqslant2$，则 a 为奇数.

若 d 为偶数，则 $a^d+1\equiv2\pmod 4$，不可能，故 d 为奇数.

如果 $d>1$，由于 $\dfrac{a^d+1}{a+1}=a^{d-1}-a^{d-2}+\cdots+1$ 为大于 1 的奇数，这与 $a^d+1=2^l$ 矛盾！

所以 $d=1,n=kd=2$，由 $m<n$ 知：$m=1,a=2^l-1$.

反之，当 $a=2^l-1(l\geqslant 2)$，$m=1$，$n=2$ 时，

由 $a^2-1=(a-1)(a+1)=2^l\cdot(a-1)$，知

$S(a^2-1)=S(a-1)$.

综上知，所求的 $(a,m,n)=(2^l-1,1,2)$，$l\in \mathbf{Z}^+$，$l\geqslant 2$.

例 10 （IMO－45 预选题）已知从正整数集 $\mathbf{N}_+$ 到其自身的函数 ψ 定义为

$$\psi(n)=\sum_{k=1}^{n}(k,n),n\in\mathbf{N}_+,$$

其中 (k,n) 表示 k 和 n 的最大公因数.

(1) 证明：对于任意两个互素的正整数 m,n，有 $\psi(mn)=\psi(m)\psi(n)$；

(2) 证明：对于每一个 $a\in\mathbf{N}_+$，方程 $\psi(x)=ax$ 有一个整数解；

(3) 求所有的 $a\in\mathbf{N}_+$，使得方程 $\psi(x)=ax$ 有唯一的整数解.

解 (1) 设 m,n 是两个互素的正整数，则对于任意一个 $k\in\mathbf{N}_+$，有

$(k,mn)=(k,m)(k,n)$.

$$故\ \psi(mn)=\sum_{k=1}^{mn}(k,mn)=\sum_{k=1}^{mn}(k,m)(k,n).$$

对于每一个 $k\in\{1,2,\cdots,mn\}$，有唯一的有序正整数对 (r,s) 满足

$r\equiv k(\mathrm{mod}\ m)$，$s\equiv k(\mathrm{mod}\ n)$，$1\leqslant r\leqslant m$，$l\leqslant s\leqslant n$.

这个映射是双射.

实际上，满足 $1\leqslant r\leqslant m$，$l\leqslant s\leqslant n$ 的数对 (r,s) 的个数为 mn.

如果 $k_1\equiv k_2(\mathrm{mod}\ m)$，$k_1\equiv k_2(\mathrm{mod}\ n)$，其中 $k_1,k_2\in\{1,2,\cdots,mn\}$，则

$k_1\equiv k_2(\mathrm{mod}\ mn)$.

所以，有 $k_1=k_2$.

因为对于每一个 $k\in\{1,2,\cdots,mn\}$ 和它对应的数对 (r,s)，有

$(k,m)=(r,m)$；$(k,n)=(s,n)$.

$$则\ \psi(mn)=\sum_{k=1}^{mn}(k,m)(k,n)=\sum_{\substack{1\leqslant r\leqslant m\\ l\leqslant s\leqslant n}}(r,m)(s,n)$$

$$=\sum_{r=1}^{m}(r,m)\sum_{s=1}^{n}(s,n)=\psi(m)\psi(n).$$

(2) 设 $n=p^\alpha$，其中 p 是素数，α 是正整数. $\sum\limits_{k=1}^{n}(k,n)$ 中的每一个被加数都具有 p^l 的形式，p^l 出现的次数等于区间 $[1,p^\alpha]$ 中能被 p^l 整除但不能被 p^{l+1} 整除的整数的个数.

于是，对于 $l=0,1,\cdots,\alpha-1$，这些整数的个数为 $p^{\alpha-l}-p^{\alpha-l-1}$. 所以，

$$\psi(n)=\psi(p^{\alpha})=p^{\alpha}+\sum_{l=0}^{\alpha-1}p^{l}(p^{\alpha-l}-p^{\alpha-l-1})$$
$$=(\alpha+1)p^{\alpha}-\alpha p^{\alpha-1}. \qquad ①$$

对于任意的 $a\in\mathbf{N}_{+}$，取 $p=2,\alpha=2a-2$，有

$\psi(2^{2a-2})=a\cdot 2^{2a-2}$.

所以，$x=2^{2a-2}$ 是方程 $\psi(x)=ax$ 的一个整数解.

(3) 取 $\alpha=p$，可得 $\psi(p^{p})=p^{p+1}$，其中 p 为素数. 如果 $a\in\mathbf{N}_{+}$ 有一个奇素因数 p，则 $x=2^{\frac{2a}{p}-2}p^{p}$ 满足方程 $\psi(x)=ax$.

实际上，由 (1) 及式①可得

$$\psi(2^{\frac{2a}{p}-2}p^{p})=\psi(2^{\frac{2a}{p}-2})\psi(p^{p})=\frac{2a}{p}\cdot 2^{\frac{2a}{p}-3}p^{p+1}=a\cdot 2^{\frac{2a}{p}-2}p^{p}.$$

因为 p 是奇数，所以，解 $x=2^{\frac{2a}{p}-2}p^{p}$ 和 $x=2^{2a-2}$ 不同.

于是，若 $\psi(x)=ax$ 有唯一的整数解，则 $a=2^{\alpha},\alpha=0,1,2,\cdots$.

下面证明，反之结论也是正确的.

考虑 $\psi(x)=2^{\alpha}x$ 的任意整数解 x，设 $x=2^{\beta}l$，其中 $\beta\geqslant 0$，l 是奇数. 由 (1) 及式①可得

$$2^{\alpha+\beta}l=2^{\alpha}x=\psi(x)=\psi(2^{\beta}l)=\psi(2^{\beta})\psi(l)=(\beta+2)2^{\beta-1}\psi(l).$$

由于 l 是奇数，由 ψ 的定义，可得 $\psi(l)$ 是奇数个奇数的和，还是奇数. 所以 $\psi(l)$ 整除 l.

又由 $\psi(l)>l(l>1)$，可得 $l=1=\psi(l)$.

于是，有 $\beta=2^{\alpha+1}-2=2a-2$，即 $x=2^{2a-2}$ 是方程 $\psi(x)=ax$ 的唯一整数解.

因此，$\psi(x)=ax$ 有唯一的整数解当且仅当 $a=2^{\alpha},\alpha=0,1,2,\cdots$.

2. 善于运用欧拉函数的性质

例 11 (IMO-32 试题)设 n 是大于 6 的整数，且 $a_1,a_2,\cdots,a_k$ 是所有小于 n 且与 n 互素的自然数，如果 $a_2-a_1=a_3-a_2=\cdots=a_k-a_{k-1}>0$，求证 n 或者是素数或者是 2 的某个正整数次幂.

证明 显然 $a_1=1$.

因为 $(n-1,n)=1$，所以 $a_k=n-1$.

令 $d=a_2-a_1>0$.

(1) 当 $a_2=2$ 时，$d=1$.

从而 $a_i=i,a_k=k=n-1$.

由已知，$a_1=1,a_2=2,\cdots,a_k=k$ 是所有与 $n=k+1$ 互素的自然数，因而 n 是素数.

(2) 当 $a_2=3$ 时，$d=2$.

此时 $a_3=5, a_4=7, \cdots$，从而 $a_1, a_2, \cdots, a_k$ 都是奇数，$n-k+1$ 是偶数.

因为 n 与小于 n 的奇数互素，所以 n 是 2 的某个正整数次幂.

(3) 当 $a_2>3$ 时，首先 a_2 不可能是合数.

若 a_2 是合数，则 $a_2=pq, p>1, q>1$.

因为 $(a_2, n)=1$，则 $(pq, n)=1$，即有 $(p, n)=1, (q, n)=1$.

于是 p, q 应为 $\{a_1, a_2, \cdots, a_k\}$ 中的两个元素，而 $p<a_2, q<a_2$，这是不可能的.

所以 a_2 是不能整除 n 的最小素数.

因为 $a_2>3$，所以 3 与 n 不可能再互素，于是必有 $3 \mid n$.

由于存在自然数 m，使得 $n-1=a_k=1+md$，所以

$n=2+md$.

即有 $3 \nmid d$.

因为 $a_2=1+d, 3 \nmid a_2$，所以 $3 \nmid 1+d$.

于是 d 满足 $d \equiv 1 \pmod 3$.

所以有 $3 \mid 1+2d$.

如果 $1+2d<n$，则 $a_3=1+2d$，此时有

$(a_3, n) \geqslant 3$.

与 $(a_3, n)=1$ 矛盾.

如果 $1+2d \geqslant n$，则必有

$n-1=1+d$.

即小于 n 且与 n 互素的自然数只有 $a_1=1, a_2=1+d$，即其个数 $\varphi(n)=2$.

令 $n=p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$，其中 $p_1<p_2<\cdots<p_t$，且是素数，$\alpha_i, i=1,2,\cdots,t$ 是自然数，则由欧拉函数性质可得 $\varphi(n)=\prod\limits_{i=1}^{t} p_i^{\alpha_i-1}(p_i-1)$.

由 $\varphi(n)=2$ 可得 $n=3$，或 4，与 $a_2>3$ 矛盾.

综上所述，n 是素数或是 2 的某个正整数次幂.

例 12 (2006 年伊朗国家队选拔考试题)设 p 是一个素数，求所有自然数 n，使得 $p \mid \varphi(n)$，且对所有满足 $(a, n)=1$ 的 a，有 $n \mid (a^{\frac{\varphi(n)}{p}}-1)$.

解 设 $n=\prod\limits_{i=1}^{m} p_i^{\alpha_i}$，则 $\varphi(n)=\prod\limits_{i=1}^{m} \varphi(p_i^{\alpha_i})=\prod\limits_{i=1}^{m}[p_i^{\alpha_i-1}(p_i-1)]$.

显然，$p \mid \varphi(n)$ 的充要条件是，存在某个 $p_i=p$ 或某个 p_i 满足 $p \mid (p_i-1)$.

而对任意的 $a, (a, n)=1$，有

$n \mid (a^{\frac{\varphi(n)}{p}}-1) \Leftrightarrow p_i^{\alpha_i} \mid (a^{\frac{\varphi(n)}{p}}-1)(i=1,2,\cdots,m) \Leftrightarrow \varphi(p_i^{\alpha_i}) \left| \frac{\varphi(n)}{p} \right.(i=1,2,\cdots,m)$.

下面分情况讨论：

(1) 至少有两个 p_k, p_l 满足 $p\mid(p_k-1), p\mid(p_l-1)$.

则 $\frac{\varphi(p_k^{\alpha_k})}{p}\in\mathbf{N}_+, \frac{\varphi(p_l^{\alpha_l})}{p}\in\mathbf{N}_+$.

故 $\varphi(p_i^{\alpha_i})\left|\frac{\varphi(n)}{p}\right.(i=1,2,\cdots,m)$, n 满足条件.

(2) 恰有一个 p_k, 满足 $p\mid(p_k-1)$.

设 $p^a\parallel\varphi(p_k^{\alpha_k})(a\in\mathbf{N}_+)$.

(i) $p\nmid n$, 此时, $p^{a-1}\parallel\frac{\varphi(n)}{p}$, 与 $\varphi(p_k^{\alpha_k})\left|\frac{\varphi(n)}{p}\right.$ 矛盾. 故 n 不满足条件.

(ii) $p\mid n$, 不妨设 $p_1=p$.

若 $\alpha_1\geqslant 2$, 则 $\frac{\varphi(p_1^{\alpha_1})}{p}\in\mathbf{N}_+, \frac{\varphi(p_k^{\alpha_k})}{p}\in\mathbf{N}_+$, 故 $\varphi(p_i^{\alpha_i})\left|\frac{\varphi(n)}{p}\right.(i=1,2,\cdots,m)$, n 满足条件.

若 $\alpha_1=1$, 此时 $p^{a-1}\parallel\frac{\varphi(n)}{p}$, 与 $\varphi(p_k^{\alpha_k})\left|\frac{\varphi(n)}{p}\right.$ 矛盾. 故 n 不满足条件.

(3) 没有 p_k 满足 $p\mid(p_k-1)$, 则 $p\mid n$.

不妨设 $p_1=p$.

此时 $p^{\alpha_1-1}\parallel\varphi(p_1^{\alpha_1})$, 但 $p^{\alpha_1-2}\parallel\frac{\varphi(n)}{p}$, 与 $\varphi(p_1^{\alpha_1})\left|\frac{\varphi(n)}{p}\right.$ 矛盾. 故 n 不满足条件.

例 13 (2004 年西部数学奥林匹克题)设 $n\in\mathbf{N}_+$, 用 $d(n)$ 表示 n 的所有正约数的个数, $\varphi(n)$ 表示 $1,2,\cdots,n$ 中与 n 互素的数的个数. 求所有的非负整数 c, 使得存在正整数 n, 满足 $d(n)+\varphi(n)=n+c$, 并且对这样的每一个 c, 求出所有满足上式的正整数 n.

解 设 n 的所有正约数组成的集合为 A, $1,2,\cdots,n$ 中与 n 互素的数组成的集合为 B. 由于 $1,2,\cdots,n$ 中恰好有一个数 $1\in A\cap B$, 所以 $d(n)+\varphi(n)\leqslant n+1$, 故 $c=0$ 或 1.

(1) 当 $c=0$ 时, 由 $d(n)+\varphi(n)=n$ 知, $1,2,\cdots,n$ 中恰好有一个不属于 $A\cup B$. 如果 n 为偶数, 且 $n>8$, 则 $n-2, n-4$ 都不属于 $A\cup B$, 此时 n 不满足方程; 如果 n 为奇数, 则当 n 为素数或 1 时, $d(n)+\varphi(n)=n+1$[属于情形 (2)], 当 n 为合数时, 设 $n=pq$, $1<p\leqslant q$, p, q 都是奇数, 若 $q\geqslant 5$, 则 $2p, 4p$ 不属于 $A\cup B$, 此时 n 不满足方程.

综上可知, 只有当 $n\leqslant 8$, n 为偶数, 或 $n\leqslant 9$, n 为奇合数, 才有 $d(n)+\varphi(n)=n$, 直接验证可知: n 只能是 6, 8 和 9.

(2) 当 $c=1$ 时, 由 $d(n)+\varphi(n)=n+1$ 知, $1,2,\cdots,n$ 中每个数都属于 $A\cup B$, 易知, 此时 $n=1$ 或素数都符合要求. 对于 n 为偶数(非素数)时的情形, 同上讨论可知, $n\leqslant 4$(考虑数 $n-2$ 即可); 若 n 为奇合数, 设 $n=pq$, $3\leqslant p\leqslant q$, p, q 都是奇数, 这时 $2p\notin A\cup B$, 矛盾. 直接验证知, $n=4$ 符合要求.

所以, 满足 $d(n)+\varphi(n)=n+1$ 的 n 为 1, 4 或素数.

注 $A\cap B=\{1\}$是显然的，故 $c\leqslant 1$. 当 n 为素数时，易知 $d(n)+\varphi(n)=n+1$；当 n 为合数时，对充分大的合数 n，找到足够数量的小于 n 的合数，使之既非 n 的约数，又不与 n 互素是容易的，这时 $d(n)+\varphi(n)\neq n+c(c=0$ 或 $1)$. 此问题的一般情形是取消整数 c 为"非负"的限制.

【模拟实战】

1. (IMO－24 试题)设 a,b,c 为两两互素的正整数. 证明 $2abc-ab-bc-ca$ 是不能表示为 $xbc+yca+zab$ 形式的最大整数(其中 x,y,z 是非负整数).
2. (IMO－33 预选题)证明对任何整数 m，存在无穷多组整数 (x,y)，使得
   (1) x 与 y 互素；
   (2) y 整除 x^2+m；
   (3) x 整除 y^2+m.
3. (1990 年第 19 届美国数学奥林匹克题)假设项链 A 有 14 个珠，B 有 19 个珠. 证明对于每一个奇数 $n\geqslant 1$，能够找到一种方法，使之能用数组 $\{n,n+1,n+2,\cdots,n+32\}$ 中的数给每个珠标上一个数，使得每个数恰好用上一次，且相邻的珠子标的数互素. (这里一个项链可以看成是一些珠围成的一个圆，其中每个珠与另外两个珠相邻)
4. 以 $\varphi(n)$ 表示与自然数 n 互素且小于 n 的自然数的个数.
   (1) p,q 是两相异的素数，证明 $\varphi(pq)=(p-1)(q-1)$.
   (2) 利用 (1) 的结论，求满足 $\varphi(pq)=3p+q$ 时的 p,q 之值.
5. (1988 年加拿大数学奥林匹克训练题)序列 $\{S_n\}$ 构造如下：$S_1=\{1,1\}$，$S_2=\{1,2,1\}$，$S_3=\{1,3,2,3,1\}$，一般地，若 $S_k=\{a_1,a_2,\cdots,a_n\}$，则 $S_{k+1}=\{a_1,a_1+a_2,a_2,a_2+a_3,\cdots,a_{n-1}+a_n,a_n\}$. 在 S_{1988} 中有多少项等于 1988?
6. (IMO－47 预选题)已知 $x\in(0,1)$，令 $y\in(0,1)$，且 y 的小数点后第 n 位数字是 x 的小数点后第 2^n 位数字. 证明：若 x 是有理数，则 y 也是有理数.
7. 证明：不存在非负整数 k 和 m，使得 $k!+48=48(k+1)^m$.

第十二章 欧拉定理、费马小定理

【基础知识】

1. 欧拉定理

设 $m\geqslant 2$，且 $(a,m)=1$，$\varphi(m)$ 为欧拉函数，则 $a^{\varphi(m)}\equiv 1(\text{mod } m)$.

事实上，若设 $r_1,r_2,\cdots,r_{\varphi(m)}$ 是模 m 的一个简化剩余系，由于 $(a,m)=1$，所以 ar_1，$ar_2,\cdots,ar_{\varphi(m)}$ 也是模 m 的一个简化剩余系.

所以 $ar_1\cdot ar_2\cdot\cdots\cdot ar_{\varphi(m)}\equiv r_1r_2\cdots r_{\varphi(m)}(\text{mod } m)$，即 $m\mid(a^{\varphi(m)}-1)r_1r_2\cdots r_{\varphi(m)}$.

又 $(m,r_1r_2\cdots r_{\varphi(m)})=1$，所以 $m\mid a^{\varphi(m)}-1$，故 $a^{\varphi(m)}\equiv 1(\text{mod } m)$.

2. 定义

设 $m>1$ 是一个固定的整数，a 是与 m 互素的整数，存在整数 k，$1\leqslant k\leqslant m$，使 $a^k\equiv 1(\text{mod } m)$，则称具有这一性质的最小正整数（仍记为 k）为 a 模 m 的阶.

a 模 m 的阶 k 具有如下性质：

(1) 设 $(a,m)=1$，k 是 a 模 m 的阶，u，v 是任意整数，则 $a^u\equiv a^v(\text{mod } m)$ 的充要条件是 $u\equiv v(\text{mod } k)$.

特别地，$a^u\equiv 1(\text{mod } k)$ 的充要条件是 $k\mid u$.

(2) 设 $(a,m)=1$，a 模 m 的阶为 k，则数列 $a,a^2,\cdots,a^k,a^{k+1},\cdots$ 是模 m 的周期数列，其最小正周期为 k，而 k 个数 $a,a^2,\cdots,a^k$ 模 m 互不同余.

(3) 设 $(a,m)=1$，则 a 模 m 的阶整除欧拉函数 $\varphi(m)$.

3. 费马小定理

设 p 是素数，且 $(a,p)=1$，则 $a^{p-1}\equiv 1(\text{mod } p)$.

注：(1) 对于任意的整数 a 和任意的素数 p，有 $a^p\equiv a(\text{mod } p)$.

事实上，若 $(a,p)\neq 1$，则 $p\mid a$，这时结论显然成立. 若 $(a,p)=1$，则由欧拉定理，有 $a^{\varphi(p)}\equiv 1(\text{mod } p)$，又 $\varphi(p)=p-1$，所以 $a^{p-1}\equiv 1(\text{mod } p)$.

(2) 费马小定理是欧拉定理当 m 为素数时的特例.

(3) 费马小定理的逆命题不成立，即使得 $2^n\equiv 2(\text{mod } n)$ 成立的 n 并不一定是素数. 能使此式成立的合数 n 称为伪素数.

【典型例题与基本方法】

例 1 证明 341 是伪素数.

证明 因 $341=11\cdot 31$ 是合数. 由费马小定理得

$2^{11}\equiv 2 \pmod{11}$，$2^{31}\equiv 2 \pmod{31}$，所以

$2^{341}=(2^{11})^{31}\equiv 2^{31}=2^9\cdot(2^{11})^2\equiv 2^9\cdot 2^2=2^{11}\equiv 2 \pmod{11}$，

及 $2^{341}=(2^{31})^{11}\equiv 2^{11}=2\cdot 1024\equiv 2\cdot 1\equiv 2 \pmod{31}$.

由以上二式即得 $2^{341}\equiv 2 \pmod{341}$，即说明 341 是伪素数.

例 2 （2005 年德国数学奥林匹克题）设 $Q(n)$ 表示正整数 n 的各位数字之和. 证明：$Q(Q(Q(2005^{2005})))=7$.

证明 显然 $Q(n)\equiv n \pmod 9$.

而 $2005^{2005}\equiv(9\times 222+7)^{2005}\equiv 7^{2005}=7^{6\times 334+1} \pmod 9$.

由欧拉定理，

$7^{\varphi(9)}=7^6\equiv 1 \pmod 9$.

所以，$2005^{2005}\equiv 7 \pmod 9$.

故 $Q(Q(Q(2005^{2005})))\equiv 2005^{2005}\equiv 7 \pmod 9$.

又 $2005^{2005}<(10^4)^{2005}=10^{8020}$，所以，$2005^{2005}$ 至多有 8020 位.

故 $Q(2005^{2005})\leqslant 9\times 8020=72180$.

于是，$Q(2005^{2005})$ 至多只有 5 位.

因此，$Q(Q(2005^{2005}))\leqslant 9\times 5=45$.

从而，$Q(Q(Q(2005^{2005})))\leqslant 3+9=12$.

又 $Q(Q(Q(2005^{2005})))\equiv 7 \pmod 9$，所以，$Q(Q(Q(2005^{2005})))=7$.

例 3 （1990 年国家集训队训练题）求出所有小于 10 的正整数 M，使得 5 整除 1989^M+M^{1989}.

解 考虑 mod 5.

$1989^M\equiv(-1)^M \pmod 5$.

若 $M=5$，则 $M^{1989}=5^{1989}\equiv 0 \pmod 5$，$1989^M=1989^5\equiv -1 \pmod 5$，则

$5\nmid 1989^M+M^{1989}$.

于是 $M\neq 5$.

由费马小定理，5 是素数，又 $M\neq 5$ 且 $1\leqslant M\leqslant 9$，则 $(5,M)=1$，于是

$M^{1989}\equiv M \pmod 5$.

若 M 为奇数，则 $5\mid M-1$，因而 $M=1$.

若 M 为偶数，则 $5\mid M+1$，因而 $M=4$.

于是 $M=1$ 或 4.

例 4 求 7^{10000} 与 7^{9999} 的末三位数字.

解 求一个数的末三位数字,就是求这个数除以 1000 的余数.

因为 $\varphi(1000)=\varphi(2^3\cdot 5^3)=2^2\cdot 5^2\cdot 4=400$.

所以,由欧拉定理,有 $7^{400}\equiv 1\pmod{1000}$.

从而 $7^{10000}\equiv 7^{400\cdot 25}\equiv 1^{25}\equiv 1\pmod{1000}$,即

7^{10000} 的末三位数字为 0,0,1.

因为 $7\cdot 7^{9999}=7^{10000}\equiv 1\equiv 1001\pmod{1000}$,所以

$7^{9999}\equiv\dfrac{1001}{7}\equiv 143\pmod{1000}$.

故 7^{9999} 的末三位数字为 1,4,3.

注 为了求 7^{9999} 的末三位数字,应当先求 7^{10000} 的末三位数字.因为后者可借助欧拉定理很快求出结果.

例 5 (第 34 届美国数学奥林匹克题)证明:方程组 $\begin{cases}x^6+x^3+x^3y+y=147^{157},\\ x^3+x^3y+y^2+y+z^9=157^{147}\end{cases}$ 没有整数解.

证明 将方程两端相加,再同时加上 1,可得

$(x^3+y+1)^2+z^9=147^{157}+157^{147}+1.$ ①

下面证明,式①两边模 19 不同余.

选择模 19 是因为 2 和 9 的最小公倍数为 18,由费马小定理,当 a 不是 19 的倍数时,$a^{18}\equiv 1\pmod{19}$.

特别地,$(z^9)^2\equiv 0$ 或 $1\pmod{19}$,于是,有

$z^9\equiv -1,0,1\pmod{19}$.

经计算可得

$n^2\equiv -8,-3,-2,0,1,4,5,6,7,9\pmod{19}$.

由费马小定理有

$147^{157}+157^{147}+1\equiv 147^{13}+157^3+1\equiv -5^{13}+5^3+1\equiv 14\pmod{19}$.

因为 $z^9+n^2\not\equiv 14\pmod{19}$,所以,式①无整数解.

例 6 (CMO-24 试题)求所有的素数对(p,q),使得 $pq\mid(5^p+5^q)$.

解 若 $2\mid pq$,不妨设 $p=2$,则 $2q\mid(5^2+5^q)\Rightarrow q\mid(5^q+25)$.

由费马小定理知 $q\mid(5^q-5)$,得 $q\mid 30$,即 $q=2,3,5$.

易验证素数对(2,2)不合要求,(2,3),(2,5)符合要求.

若 pq 为奇数且 $5\mid pq$,不妨设 $p=5$,则

$5q\mid(5^5+5^q)\Rightarrow q\mid(5^{q-1}+625)$.

当 $q=5$ 时，素数对 $(5,5)$ 符合要求.

当 $q\neq5$ 时，由费马小定理有 $q\mid(5^{q-1}-1)$，故 $q\mid626$. 由于 q 为奇素数，而 626 的奇素因子只有 313，所以，$q=313$.

经检验，素数对 $(5,313)$ 符合要求.

若 p,q 都不等于 2 和 5，则 $pq\mid(5^{p\ 1}+5^{q-1})$，故

$5^{p-1}+5^{q-1}\equiv0(\bmod p)$. ①

由费马小定理得

$5^{p-1}\equiv(\bmod p)$. ②

由式①，②得

$5^{q-1}\equiv-1(\bmod p)$. ③

设 $p-1=2^k(2r-1)$，$q-1=2^l(2s-1)$（k,l,r,s 为正整数）.

若 $k\leqslant l$，则由式②，③易知

$$1=1^{2^{l-k}(2s-1)}\equiv(5^{p-1})^{2^{l-k}(2s-1)}$$

$$\equiv5^{2^l(2r-1)(2s-1)}=(5^{q-1})^{2r-1}$$

$$\equiv(-1)^{2r-1}\equiv-1(\bmod p),$$

这与 $p\neq2$ 矛盾. 因此，$k>l$.

同理，$k<l$，矛盾.

此时不存在符合要求的 (p,q).

综上，满足题目要求的素数对 (p,q) 为 $(2,3)$，$(3,2)$，$(2,5)$，$(5,2)$，$(5,5)$，$(5,313)$，$(313,5)$.

例 7 （1988 年加拿大数学奥林匹克训练题）设整数 k 不能被 5 整除，证明 x^5-x+k 不能写成两个次数较低的整系数多项式的乘积.

证明 对 x^5-x+k 的分解有两种可能：

$x^5-x+k=(x+a)(x^4+bx^3+cx^2+dx+e)$,

$x^5-x+k=(x^2+ax+b)(x^3+cx^2+dx+e)$.

上两式的字母系数都是整数.

对于第一种可能：

$-a$ 为 x^5-x+k 的根，所以有 $-(a^5-a)+k=0$.

由费马小定理，$5\mid a^5-a$.

从而 k 能被 5 整除，与 k 不能被 5 整除矛盾.

对于第二种可能：

比较等式两边同次项系数，得

$a+c=0$,

$ac+b+d=0$

$e+ad+bc=0$,

$ae+bd=-1$,

$be=k$.

由前二式得 $c=-a, d=a^2-b, e=2ab-a^3$,代入后两式得

$3a^2b+1=a^4+b^2, ab(2b-a^2)=k$.

于是有

$k=2a(3a^2b+1-a^4)-a^3b=-2(a^5-a)+5a^3b$.

仍由费马小定理,$5|a^5-a$,从而 k 能被 5 整除,与 k 不能被 5 整除矛盾.

所以在 k 不能被 5 整除时,x^5-x+k 不能分解成两个次数较低的整系数多项式的积.

例 8 (IMO-40 试题)确定所有的正整数对 (n,p),满足:

p 是一个素数,$n\leqslant 2p$,且 $(p-1)^n+1$ 能够被 n^{p-1} 整除.

解 当 $n=1$ 时,由于 $(p-1)^n+1=p$,显然能被 $1^{p-1}=1$ 整除,于是 $(n,p)=(1,p)$ 是一组解.

当 $n=2$ 时,由于 $(p-1)^2+1=p^2+2p+2$,若能被 2^{p-1} 整除,必须 p^2 为偶数,又 p 是素数,于是 $p=2$,于是 $(n,p)=(2,2)$ 是另一组解.

下面考虑 $n\geqslant 2, p\geqslant 3$ 的情形.

当素数 $p\geqslant 3$ 时,$(p-1)^n+1$ 是奇数,若能被 n^{p-1} 整除,则 n 也是奇数,$n\neq 2p$,从而,$n<2p$.

记 q 为 n 的最小素因子,则由 $n^{p-1}|(p-1)^n+1$,可知

$q|(p-1)^n+1, (p-1)^n\equiv -1 \pmod q$,且 $(q,p-1)=1$.

由 q 的选取可知 $(n,p-1)=1$.

于是存在整数 u,v,使得 $un+v(q-1)=1$.

由 Fermat 小定理,$q|(p-1)^{q-1}-1$,于是

$p-1\equiv(p-1)^1=(p-1)^{un}\cdot(p-1)^{v(q-1)}\equiv(-1)^u\cdot 1^v \pmod q$.

由 $q-1$ 为偶数,n 为奇数可知 u 为奇数,从而

$p-1\equiv -1 \pmod q$,即 $p\equiv 0 \pmod q$.

这表明 $q|p$,进而有 $p|q$,即证得 $q=p$.

于是可以得到 $p^{p-1}|(p-1)^p+1=p^2(p^{p-2}-C_p^1p^{p-3}+\cdots+C_p^{p-3}p-C_p^{p-2}+1)$.

上式中括号内,除最后一项是 1 之外,其余各项均能被 p 整除.

从而 $p-1\leqslant 2$,即 $p=3$,此时 $n=3$.

所以 $(n,p)=(3,3)$ 是一组解.

本题有三组解$(n,p)=(1,p),(2,2),(3,3)$.

例 9 (2007 年意大利国家队选拔考试题)p 为大于 3 的素数,证明:

(1) $(p-1)^p+1$ 至少含有一个不同于 p 的素因子;

(2) 设$(p-1)^p+1=\prod_{i=1}^{n}p_i^{\alpha_i}$,其中,$p_1,p_2,\cdots,p_n$ 是互不相同的素数,$\alpha_1,\alpha_2,\cdots,\alpha_n$ 为正整数,则 $\sum_{i=1}^{n}p_i\alpha_i\geqslant\frac{p^2}{2}$.

证明 (1) 因为

$$\begin{aligned}(p-1)^p+1&=(p-1+1)[(p-1)^{p-1}-(p-1)^{p-2}+(p-1)^{p-3}-\cdots\\&\quad+(p-1)^2-(p-1)+1]\\&=p\sum_{i=0}^{p-1}(-1)^i(p-1)^i\\&=p[1+(p-2)\sum_{j=1}^{\frac{p-1}{2}}(p-1)^{2j-1}]\\&>p(1+2\times\frac{p-1}{2})=p^2,\end{aligned}$$

又

$$\begin{aligned}\sum_{i=0}^{p-1}(-1)^i(p-1)^i&\equiv\sum_{i=0}^{p-1}(1-ip)\equiv p-p\sum_{i=0}^{p-1}i\\&\equiv p-p\times\frac{p(p-1)}{2}\equiv p\pmod{p^2},\end{aligned}$$

所以,$(p-1)^p+1$ 含有不同于 p 的素因子.

(2) 假设 $q(\neq p)$是$(p-1)^p+1$ 的另一个素因子,易知 $q\neq2$,则

$(p-1)^{2p}\equiv1\pmod q$.

又因为 $q\mid[(p-1)^p+1]$,所以$(p-1,q)=1$.

故由费马小定理得$(p-1)^{q-1}\equiv1\pmod q$.

设$(q-1,2p)=d$,则由$(p-1)^{2p}\equiv1\pmod q$,$(p-1)^{q-1}\equiv1\pmod q$,得

$(p-1)^d\equiv1\pmod q$.

这是因为,一定存在正整数 s,满足

$s=\min\{x\in\mathbf{Z}_+\mid(p-1)^x\equiv1\pmod q\}$.

设 $2p=as+b(0\leqslant b\leqslant s-1)$,则由$(p-1)^{2p}\equiv(p-1)^{as+b}\equiv(p-1)^b\pmod q$及 s 的定义知 $b=0$,即 $s\mid 2p$.

同理,$s\mid(q-1)$.

所以,$s\mid(2p,q-1)$.

故$(p-1)^d\equiv1\pmod q$.

又因为$(q-1,2p)=d$，所以，d 为 $1,2,p$ 或 $2p$.

(i) 若 $d=1$ 或 p，则$(p-1)^p\equiv1 \pmod q$，与 $q\mid[(p-1)^p+1]$矛盾.

(ii) 若 $d=2$，则$(p-1)^2\equiv1 \pmod q$，故

$(p-1)^{p-1}\equiv1 \pmod q$，

$(p-1)^p\equiv(p-1) \pmod q$.

由此知，$(p-1)^p+1\equiv p \pmod q$，矛盾.

因此，必有 $d=2p$.

于是，$2p\mid(q-1)$，得 $q>p$.

设$(p-1)^p+1$ 的所有素因子为 $p_i(i=1,2,\cdots,n)$.

令 $\beta_i=\alpha_i\log_p p_i$，则 $p_i^{\alpha_i}=p^{\beta_i}$.

由于函数 $x\mapsto\frac{x}{\ln x}$在$[e,+\infty)$上单调递增，则

$$\alpha_i p_i=\beta_i\ln p\cdot\frac{p_i}{\ln p_i}\geqslant\beta_i\ln p\,\frac{p}{\ln p}=\beta_i p.$$

因此，$\sum\limits_{i=1}^{n}\alpha_i p_i\geqslant p\sum\limits_{i=1}^{n}\beta_i$.

此外，由于

$$\sum_{i=1}^{n}\beta_i=\sum_{i=1}^{n}\alpha_i\log_p p_i=\log_p[(p-1)^p+1]\geqslant p\log_p(p-1)\geqslant\frac{p}{2},$$

故$\sum\limits_{i=1}^{n}\alpha_i p_i\geqslant p\sum\limits_{i=1}^{n}\beta_i\geqslant\frac{p^2}{2}$.

【解题思维策略分析】

1. 灵活运用欧拉定理

例 10 (2005 年国家队集训测试题)设 $a_0,a_1,\cdots,a_n,x_0,x_1,\cdots,x_n(n\geqslant2)$均为整数，$r(\geqslant2)$为整数，满足 $\sum\limits_{j=0}^{n}a_jx_j^k=0,k=1,2,\cdots,r$.

证明：对正整数 $m\in\{r+1,r+2,\cdots,2r+1\}$，都有 $\sum\limits_{j=0}^{n}a_jx_j^m\equiv0 \pmod m$.

证明 任取 $p^\alpha\parallel m$，其中 p 是素数，$\alpha\geqslant1$，则由 $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$，知

$\varphi(p^\alpha)\ \left(m-\frac{m}{p}\right)$.

因为$\frac{m}{p}\leqslant\frac{2r+1}{2}<r+1$，所以$\frac{m}{p}\leqslant r$，于是 $r\geqslant\frac{m}{p}\geqslant p^{\alpha-1}\geqslant\alpha$.

对任意 x_j，$j=0,1,2,\cdots,n$，若 $p\mid x_j$，则由 $m>\frac{m}{p}\geqslant\alpha$ 得 $x_j^m\equiv x_j^{\frac{m}{p}}\pmod{p^\alpha}$；若 $p\nmid x_j$，则由 $\varphi(p^\alpha)\left|\left(m-\frac{m}{p}\right)\right.$ 和欧拉定理，得 $x_j^{m-\frac{m}{p}}\equiv 1\pmod{p^\alpha}$. 从而也有

$x_j^m\equiv x_j^{\frac{m}{p}}\pmod{p^\alpha}$，$j=0,1,2,\cdots,n$.

因为 $\frac{m}{p}\leqslant r$，所以由上式及题设可得

$$\sum_{j=0}^{n}a_jx_j^m\equiv\sum_{j=0}^{n}a_jx_j^{\frac{m}{p}}\equiv 0\pmod{p^\alpha}.$$

由于上式对任意 $p^\alpha\parallel m$ 成立，故 $m\left|\sum_{j=0}^{n}a_jx_j^m\right.$，从而命题得证.

例 11 （2006 年国家队集训测试题）求所有的正整数对 (a,n)，使得 $\frac{(a+1)^n-a^n}{n}$ 是整数.

解 若 a 为任意正整数，则 $(a,1)$ 显然是原问题的解. 下面我们证明原问题没有其他解.

假设 $(a,n)(n\geqslant 2)$ 是原问题的一个解，则存在某正整数 k，使得

$(a+1)^n-a^n=kn$.

由于 a 和 $a+1$ 互素，由上面的方程可知，n 肯定和 a，$a+1$ 都互素.

由欧拉定理可得

$(a+1)^{\varphi(n)}\equiv a^{\varphi(n)}\equiv 1\pmod n$.

令 $d=\gcd(n,\varphi(n))$. 由 Bezout 不等式，存在整数 α 和 β 使得 $d=\alpha n+\beta\varphi(n)$.

由 $(a+1)^n\equiv a^n\pmod n$ 和 $(a+1)^{\varphi(n)}\equiv a^{\varphi(n)}\equiv 1\pmod n$ 可推出

$(a+1)^d\equiv(a+1)^{\alpha n+\beta\varphi(n)}\equiv a^{\alpha n+\beta\varphi(n)}\equiv a^d\pmod n$.

显然 $d>1$（否则 $a+1\equiv a\pmod n$ 推出 $n=1$）. 同时注意到 $\varphi(n)<n$，所以 $d<n$. 因此 (a,d) 是原问题的另一个解，并且 $1<d<n$. 重复上述过程，我们就得到了一个无穷递降正整数序列，而这是不可能的，因此上面的假设是错误的，即没有 $n>1$ 的解.

例 12 （1991 年国家集训队测验题）设 d,a,n 为自然数，且 $3\leqslant d\leqslant 2^{n+1}$，求证 $d\nmid a^{2^n}+1$.

证明 假设 $d\mid a^{2^n}+1$，则 $d\mid(a^{2^n}+1)(a^{2^n}-1)$，即

$d\mid a^{2^{n+1}}-1$. ①

显然有 $(a,d)=1$. ②

考虑以 d 为模的数列 $\{a^k\pmod d\}$. 显然由①，②可得

$d|a^{2^{n+1}+k}-a^k$，即 $a^{2^{n+1}+k}\equiv a^k(\bmod d)$.

于是 2^{n+1}是模周期数列$\{a^k(\bmod d)\}$的一个周期.

设 $T_a(d)$是$\{a^k(\bmod d)\}$的最小正周期，则 $T_a(d)|2^{n+1}$.

由欧拉定理：若$(a,m)=1$，则 $a^{\varphi(m)}\equiv1(\bmod m)$，其中 $\varphi(m)$是欧拉函数，可知 $T_a(d)|\varphi(d)$.

从而 $T_a(d)|(2^{n+1},\varphi(d))$.

注意到 $\varphi(d)\leqslant d-1$，而 $d\leqslant2^{n+1}$，所以 $\varphi(d)<2^{n+1}$.

因此$(2^{n+1},\varphi(d))\leqslant2^n$.

又$(2^{n+1},\varphi(d))|2^n$，于是 $T_a(d)|2^n$.

所以，$\{a^k(\bmod d)\}$以 2^n 为一个周期，即有 $a^{2^n}\equiv1(\bmod d)$.

于是，$a^{2^n}+1\equiv1+1\equiv2(\bmod d)$.

又由假设 $d|(a^{2^n}+1)$，从而 $2\equiv0(\bmod d)$，这与题设 $d\geqslant3$ 矛盾.

这一矛盾说明 $d\nmid(a^{2^n}+1)$.

例 13 （1993 年国家集训队选拔考试题）对素数 $p\geqslant3$，定义

$$F(p)=\sum_{k=1}^{\frac{p-1}{2}}k^{120},f(p)=\frac{1}{2}-\left\{\frac{F(p)}{p}\right\},$$

这里$\{x\}=x-[x]$表示 x 的小数部分. 求 $f(p)$的值.

解 作 120 除以 $p-1$ 的带余除法：

$120=q(p-1)+r,0\leqslant r\leqslant p-2$.

因为素数 $p\geqslant3$，所以 p 是奇数. 由于 120 与 $p-1$ 是偶数，所以 r 是偶数.

定义 $G(p)=\sum\limits_{k=1}^{\frac{p-1}{2}}k^r$.

根据费马小定理，对于 $k=1,2,\cdots,\frac{p-1}{2}$，有 $k^{p-1}\equiv1(\bmod p)$，所以

$F(p)\equiv G(p)(\bmod p)$.

$$f(p)=\frac{1}{2}-\left\{\frac{F(p)}{p}\right\}=\frac{1}{2}-\left\{\frac{G(p)}{p}\right\}.$$

以下分两种情况讨论.

情形Ⅰ：$r=0$.

此时有 $G(p)=\sum\limits_{k=1}^{\frac{p-1}{2}}k^0=\frac{p-1}{2}$.

$$f(p)=\frac{1}{2}-\left\{\frac{G(p)}{p}\right\}=\frac{1}{2}-\frac{p-1}{2p}=\frac{1}{2p}.$$

情形Ⅱ：$r\neq 0$.

因为 r 是偶数，所以对 mod p，有

$$G(p)=1^r+2^r+\cdots+\left(\frac{p-1}{2}\right)^r$$

$$\equiv(p-1)^r+(p-2)^r+\cdots+\left(p-\frac{p-1}{2}\right)^r$$

$$=(p-1)^r+(p-2)^r+\cdots+\left(\frac{p+1}{2}\right)^r \pmod p.$$

$$2G(p)=G(p)+G(p)\equiv\sum_{i=1}^{p-1}i^r \pmod p.$$

又因为同余方程 $x^r\equiv 1\pmod p$ 的互不同余的解不超过 r 个，$0\leqslant r\leqslant p-2$，所以至少存在一个 $a\in\{1,2,\cdots,p-1\}$ 使得 $a^r\not\equiv 1\pmod p$.

我们有

$2a^rG(p)=(1\cdot a)^r+(2\cdot a)^r+\cdots+((p-1)a)^r\equiv 2G(p)\pmod p$.

（这是因为 $1\cdot a,2\cdot a,\cdots,(p-1)a$ 对于 mod p 两两不同余，构成了模 p 的剩余系.）

于是 $2(a^r-1)G(p)\equiv 0\pmod p$.

又由于 $2(a^r-1)\not\equiv 0\pmod p$，所以有

$G(p)\equiv 0\pmod p$.

此时有 $f(p)=\frac{1}{2}-\left\{\frac{G(p)}{p}\right\}=\frac{1}{2}$.

下面寻求属于情形Ⅰ的素数 $p\geqslant 3$，即满足 $p-1\mid 120$ 的素数 $p\geqslant 3$. 这些素数是

3，5，7，11，13，31，41，61.

而其他素数属于情形Ⅱ.

综上所述，本题的答案为

p	3	5	7	11	13	31	41	61	其他奇素数
$f(p)$	$\frac{1}{6}$	$\frac{1}{10}$	$\frac{1}{14}$	$\frac{1}{22}$	$\frac{1}{26}$	$\frac{1}{62}$	$\frac{1}{82}$	$\frac{1}{122}$	$\frac{1}{2}$

2. 灵活运用费马小定理

例 14 （2005 年国家队培训题）求所有的整系数多项式 $f(x)$，使得对所有正整数 n，都有 $f(n)\mid 2^n-1$.

解 假设 $f(x)$ 不为常数，不妨设 $f(x)$ 首项系数为正，则存在正整数 N，使得当 $x\geqslant N$ 时，$f(x)\geqslant 2$.

任取一个正整数 n，$n\geqslant N$，取 $f(n)$ 的素因子 p，由于 $f(n)\mid 2^n-1$，所以 $2^n\equiv 1$(mod

p).

又由于 $f(n+p)\equiv f(n)\equiv 0 \pmod p$，$f(n+p)\mid 2^{n+p}-1$，所以 $2^{n+p}\equiv 1 \pmod p$，从而 $2^p=1 \pmod p$.

由费马小定理，$2^p\equiv 2 \pmod p$，从而 $1\equiv 2 \pmod p$，矛盾！

所以 $f(x)$ 为常数，设 $f(x)=a$.

由于 $f(1)\mid 2^1-1$，即 $a\mid 1$，知 $a=\pm 1$. 所以所求整系数多项式为

$f(x)=1$ 和 $f(x)=-1$.

例 15 （2006 年保加利亚国家数学奥林匹克题）设 p 是使得 p^2 能整除 $2^{p-1}-1$ 的素数. 证明：对任意自然数 n，整数 $(p-1)(p!+2^n)$ 至少有三个不同的素因子.

证明 因为 $(p-1)\mid p!$，所以，$p-1$ 和 $p!+2^n$ 的最大公因子是 2 的幂.

下面证明：$p-1$ 和 $p!+2^n$ 都至少有一个奇因子.

设 $p-1=2^k$，即 $p=2^k+1$. 若 $s\geqslant 3$ 是 k 的一个奇因子，则

$p=2^k+1=(2^t+1)A$.

所以，p 不是素数，矛盾.

因此，$k=2^t$. 由此得

$$
\begin{aligned}
2^{p-1}-1&=2^{2^k}-1=(2^{2^{k-1}}-1)(2^{2^{k-1}}+1)=\cdots\\
&=(2^{2^t}-1)(2^{2^t}+1)(2^{2^{t+1}}+1)\cdots(2^{2^{k-1}}+1).
\end{aligned}
\qquad ①
$$

因为当 $l>t$ 时，$(2^{2^l}+1,2^{2^t}+1)=1$，且 $2^{2^t}-1<p=2^{2^t}+1$，所以，p^2 不能整除式①，矛盾.

因此，$p-1$ 不是 2 的幂.

设 $p!+2^n=2^k$，则 $k>n$，且 $p!=2^n(2^{k-n}-1)$.

所以，$p\mid(2^m-1)$，其中，$m=k-n$.

设 t 是满足 $p\mid(2^t-1)$ 的最小正整数，则 $t\mid m$.

又由费马小定理知 $t\mid(p-1)$.

令 $p-1=lt$，则

$2^{p-1}-1=(2^t-1)(2^{t(l-1)}+2^{t(l-2)}+\cdots+2^t+1)$.

因为 $2^t\equiv 1 \pmod p$，则有

$2^{t(l-1)}+2^{t(l-2)}+\cdots+2^t+1\equiv l\not\equiv 0 \pmod p$.

于是，$p^2\mid(2^t-1)$，这意味着 $p^2\mid(2^m-1)$，即 $p^2\mid p!$，矛盾.

因此，$p-1$ 和 $p!+2^n$ 都至少有一个奇因子. 而这些因子是不同的，所以，$(p-1)(p!+2^n)$ 至少有三个不同的素因子.

例 16 （第 18 届亚太地区数学奥林匹克题）已知 $p(p\geqslant 5)$ 为素数. 从 $p\times p$ 的棋盘上任取 p 个方格，使得所取方格不能位于同一行（可以位于同一列），记这样的取法

数为 r. 求证：$p^5|r$.

证明 注意到 $r=C_{p^2}^{p}-p$，故只须证明

$(p^2-1)(p^2-2)\cdot\cdots\cdot[p^2-(p-1)]-(p-1)!\equiv0\pmod{p^4}$. ①

考虑多项式

$f(x)=(x-1)(x-2)\cdot\cdots\cdot[x-(p-1)]$

$\quad=x^{p-1}+s_{p-2}x^{p-2}+\cdots+s_1x+s_0$. ②

则式①等价于 $f(p^2)-s_0\equiv0\pmod{p^4}$，即 $s_1p^2\equiv0\pmod{p^4}$.

从而，$s_1\equiv0\pmod{p^2}$.

由费马小定理知，对 $a\in\{1,2,\cdots,p-1\}$，有 $a^{p-1}\equiv1\pmod p$.

则 $x^{p-1}-1\equiv(x-1)(x-2)\cdot\cdots\cdot[x-(p-1)]\pmod p$. ③

比较式③左端和式②右端各项系数，可得

$p|s_i(1\leqslant i\leqslant p-2)$，$s_0\equiv-1\pmod p$.

另一方面，在式②中，令 $x=p$，得

$s_0=f(0)=(-1)^{p-1}(p-1)!=(p-1)!=f(p)$

$\quad=p^{p-1}+s_{p-2}p^{p-2}+\cdots+s_1p+s_0$.

于是，$p^{p-1}+s_{p-2}p^{p-2}+\cdots+s_2p^2=-s_1p$.

由 $p\geqslant5$，$p|s_2$，得 $s_1\equiv0\pmod{p^2}$.

因此，结论成立.

例 17 （第 20 届韩国数学奥林匹克题）试求所有的素数对 (p,q)，使得 $pq|(p^p+q^q+1)$.

证明 显然，$p\neq q$.

不妨设 $p<q$.

当 $p=2$ 时，由 $q^q+5\equiv5\equiv0\pmod q$，知 q 只可能取 5.

经检验，知 $(p,q)=(2,5)$ 符合条件.

当 p、q 都是奇素数时，由 $p^p+1\equiv0\pmod q$，知

$q|(p^{p-1}-p^{p-2}+\cdots-p+1)$，$p^{2p}\equiv1\pmod q$.

另一方面，据费马小定理得 $p^{q-1}\equiv1\pmod q$.

若 $\gcd(2p,q-1)=2$，则 $p^2\equiv1\pmod q$，于是，$p\equiv1\pmod q$ 或 $p\equiv-1\pmod q$. 从而，

$0\equiv p^{p-1}-p^{p-2}+\cdots-p+1\equiv1$ 或 $p\pmod q$，矛盾.

若 $\gcd(2p,q-1)=2p$，即 $q\equiv1\pmod p$，则

$0\equiv p^p+q^q+1\equiv p^p+1+1\equiv2\pmod p$，同样导致矛盾.

因此，所求的所有满足条件的素数对为 $(2,5)$ 和 $(5,2)$.

例 18 （2008 年国家集训队测试题）设整数 $n>1$，n 整除 $2^{\varphi(n)}+3^{\varphi(n)}+\cdots+n^{\varphi(n)}$，记 p_1，p_2，…，p_k 是 n 的全体不同素因子. 求证：

$$\frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_k}+\frac{1}{p_1p_2\cdots p_k}$$

是整数[这里 $\varphi(n)$ 表示 1 到 n 中与 n 互素的正整数的个数].

解 设 $s_n=2^{\varphi(n)}+3^{\varphi(n)}+\cdots+n^{\varphi(n)}$. 若存在素数 p，使 $p^2\mid n$，设 $n=p^2m$，则

$$\begin{aligned}1+s_n&\equiv0^{\varphi(n)}+1^{\varphi(n)}+2^{\varphi(n)}+3^{\varphi(n)}+\cdots+(n-1)^{\varphi(n)}\\&=\sum_{j=0}^{mp-1}\sum_{k=0}^{p-1}(jp+k)^{\varphi(n)}\equiv\sum_{j=0}^{mp-1}\sum_{k=0}^{p-1}k^{\varphi(n)}\\&\equiv mp\sum_{k=0}^{p-1}k^{\varphi(n)}\equiv0\pmod p,\end{aligned}$$

即 $p\mid1+s_n$，但 $p\mid n$，$n\mid s_n$，矛盾！

所以可设 $n=p_1p_2\cdots p_k$，其中 $p_1<p_2<\cdots<p_k$ 为不同素数. 因此

$$\varphi(n)=(p_1-1)(p_2-1)\cdots(p_k-1),$$

特别地，$\varphi(n)$ 是 p_i-1 的倍数，由 Fermat 小定理得

$$x^{\varphi(n)}\equiv\begin{cases}1\pmod{p_i},(x,p_i)=1,\\0\pmod{p_i},(x,p_i)>1,\end{cases}$$

所以 $s_n\equiv n-\frac{n}{p_i}-1\pmod{p_i}$.

因为 $p_i\mid n$，$n\mid s_n$，所以 $p_i\mid1+\frac{n}{p_i}$，由此可知

$$p_1p_2\cdots p_k\mid\left(\frac{n}{p_1}+\frac{n}{p_2}+\cdots+\frac{n}{p_k}+1\right),$$

即 $p_1p_2\cdots p_k\mid p_2p_3\cdots p_k+p_1p_3\cdots p_k+\cdots+p_1p_2\cdots p_{k-1}+1$，

所以 $\frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_k}+\frac{1}{p_1p_2\cdots p_k}$ 为整数.

例 19 （1999 年第 16 届巴尔干地区数学奥林匹克题）设 $p>2$ 为素数，使得 $3\mid(p-2)$，记 $S=\{y^2-x^3-1\mid x,y\in\mathbf{Z},0\leqslant n,y\leqslant p-1\}$.

证明 S 中至多有 $p-1$ 个元素为 p 的倍数.

证明 先证明一个引论.

引理 设 $p>2$，p 为素数，且 $p\equiv2\pmod3$，则对任意整数 m,n，如果 $1\leqslant m<n\leqslant p-1$，则有 $m^3\not\equiv n^3\pmod p$.

证明引理如下：

事实上，设 $p=3k+2$，即 $p-1=3k+1$，$k\in\mathbf{N}$，又设 $m^3\not\equiv n^3\pmod p$.

设 t 是满足同余式 $m^t\equiv n^t\pmod p$ 的最小正整数，则易证对任意正整数 r，若 $m^r\equiv$

$n^r \pmod p$，则有 $t \mid r$，从而 $r \mid 3$.

另一方面，由费马小定理，$m^{p-1} \equiv 1 \pmod p$，$n^{p-1} \equiv 1 \pmod p$，则

$m^{3k+1} \equiv n^{3k+1} \pmod p$，

$\therefore r \mid (3k+1)$.

而 $r \mid 3$，则 $r=1$.

这表明 $m \equiv n \pmod p$ 与 $1 \leqslant m < n \leqslant p-1$ 矛盾.

从而引理得证.

下面证明本题.

由引理可知，当 n 跑遍 p 的一个完系时，x^3 也跑遍模 p 的一个完系. 从而，对 $0 \leqslant y \leqslant p-1$ 的每一个整数 y，都存在唯一的 $x \in \{0,1,\cdots,p-1\}$，使得

$x^3 \equiv y^2-1 \pmod p$.

这表明，集合 S 中至多只有 p 个元素是 p 的倍数.

注意到 S 中，$0=1^2-0^3-1=3^2-2^3-1$ 被表示了两次，从而 S 中至多只有 $p-1$ 个元素为 p 的倍数.

例 20 （IMO-46 预选题）求所有的正整数 $n(n>1)$，使得存在唯一的整数 $a(0<a \leqslant n!)$满足 a^n+1 可以被 $n!$ 整除.

解 n 是素数.

如果 $n=2$，则有唯一的整数 $a=1$.

如果 $n>2$，且 n 为偶数，则 a^n 是完全平方数. 因此，a^n+1 模 4 的余数为 1 或 2. 而 $n!$ 可以被 4 整除，故不存在满足条件的整数 a.

若 n 为奇数，假设 $n=p$ 是素数，且对某个正整数 $a(0<a \leqslant p!)$，使得 $p! \mid (a^p+1)$.

由费马小定理，有 $a^p+1 \equiv (a+1) \pmod p$.

因此，$p \mid (a+1)$.

下面证明：$\frac{a^p+1}{a+1}$没有小于 p 的素因数 q.

假设存在素数 $q<p$，满足 $q \left| \frac{a^p+1}{a+1} \right.$.

由于$\frac{a^p+1}{a+1} = \sum_{i=0}^{p-1}(-a)^i$ 为奇数，所以，q 为奇数.

于是，有 $a^p \equiv -1 \pmod q$.

从而，有 $a^{2p} \equiv 1 \pmod q$.

因此，a 与 q 互素，且 $a^{q-1} \equiv 1 \pmod q$.

设 $d=(q-1,2p)$，则有 $a^d \equiv 1 \pmod q$.

因为 $q<p$，所以，$d=2$，则 $a\equiv\pm1\pmod q$。

当 $a\equiv1\pmod q$ 时，有

$$\frac{a^p+1}{a+1}=\sum_{i=0}^{p-1}(-a)^i\equiv1\pmod q\text{，矛盾；}$$

当 $a\equiv-1\pmod q$ 时，有

$$\frac{a^p+1}{a+1}=\sum_{i=0}^{p-1}(-a)^i\equiv p\pmod q\text{，即 }q\mid p\text{，矛盾.}$$

由于 $\frac{a^p+1}{a+1}$ 没有小于 p 的素因数，且 $(p-1)!\mid(a+1)\left(\frac{a^p+1}{a+1}\right)$，所以

$(p-1)!\mid(a+1)$。

又因为 $p\mid(a+1)$，所以，$p!\mid(a+1)$。

于是，存在唯一的整数 $a=p!-1$。

若 n 是奇数，且为合数，设 p 为 n 的最小素因数，且 $p^\alpha\mid n!$，$p^{\alpha+1}\nmid n!$。

因为 $2p<p^2\leqslant n$，所以

$n!=1\times2\times\cdots\times p\times\cdots\times(2p)\times\cdots\times n$，且 $\alpha\geqslant2$。

设 $m=\frac{n!}{p^\alpha}$。对于任意满足 $a\equiv-1\pmod{p^{\alpha-1}m}$ 的整数 a，记

$$a=-1+p^{\alpha-1}mk. \qquad ①$$

则

$$\begin{aligned}a^p&=(-1+p^{\alpha-1}mk)^p\\&=-1+p^\alpha mk+\sum_{j=2}^{p}(-1)^{p-j}C_p^jp^{(\alpha-1)j}(mk)^j\\&=-1+p^\alpha M.\end{aligned}$$

其中，M 是整数. 这是因为对于所有的 $j\geqslant2$ 和 $\alpha\geqslant2$，均有 $(\alpha-1)j\geqslant\alpha$。

于是，$p^\alpha\mid(a^p+1)$。

从而，$p^\alpha\mid(a^n+1)$。

又因为 $m\mid(a+1)$，所以，$m\mid(a^n+1)$。

考虑到 m 与 p 互素，则对于满足式①的 a 均有 $n!\mid(a^n+1)$。但在区间 $[1,n!]$ 中有 $p(p>2)$ 个整数满足式①，即 $k=1,2,\cdots,p$，与 a 的唯一性矛盾.

例 21 （2005 年国家队集训队测试题）设 n 是正整数，$F_n=2^{2^n}+1$. 证明：对 $n\geqslant3$，数 F_n 有一个素因子大于 $2^{n+2}(n+1)$。

证明 先证一个引理.

引理 设 p 是 F_n 的任一素因子，则 p 具有形式 $2^{n+1}x_n+1$，x_n 是正整数.

引理的证明： 设 p 是 F_n 的任一素因子，则 $p\neq2$. 设 2 模 p 的阶是 k. 由

$$2^{2^n}\equiv-1\pmod p, \qquad (*)$$

得 $2^{2^{n+1}}=1 \pmod p$，故 $k \mid 2^{n+1}$，所以 k 是 2 的幂，设 $k=2^l$，其中 $0 \leqslant l \leqslant n+1$. 若 $l \leqslant n$，则将 $2^{2^l} \equiv 1 \pmod p$ 两边反复平方若干次，产生 $2^{2^n} \equiv 1 \pmod p$，结合㊅ 得 $1 \equiv -1 \pmod p$，这不可能. 故必须 $l=n+1$，即阶 $k=2^{n+1}$.

由费马小定理 $2^{p-1} \equiv 1 \pmod p$，所以 $2^{n+1} \mid p-1$，故 $p-1=2^{n+1}x_n$. 引理得证.

回到原题：设

$$F_n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \qquad ①$$

则由引理知，$p_i=2^{n+1}x_i+1$，故由①知

$$2^{2^n}+1 \geqslant (2^{n+1}+1)^{(\alpha_1+\cdots+\alpha_k)} > 2^{(n+1)(\alpha_1+\cdots+\alpha_k)}+1 \text{(用二项式展开)},$$

即有

$$\sum_{i=1}^{k} \alpha_i < \frac{2^n}{n+1}. \qquad ②$$

另一方面，由二项式展开知，

$$p_i^{\alpha_i}=(2^{n+1}x_i+1)^{\alpha_i} \equiv 1+2^{n+1}\alpha_i x_i \pmod{2^{2n+2}}.$$

由于 $n \geqslant 3$ 时，$2^n \geqslant 2n+2$，故由①模 2^{2n+2} 得到

$$1 \equiv 2^{2^n}+1=\prod_{i=1}^{k} p_i^{\alpha_i} \equiv \prod_{i=1}^{k}(1+2^{n+1}\alpha_i x_i)$$

$$\equiv 1+2^{n+1}\sum_{i=1}^{k}\alpha_i x_i \pmod{2^{2n+2}},$$

即
$$2^{n+1}\sum_{i=1}^{k}\alpha_i x_i \equiv 0 \pmod{2^{2n+2}},$$

所以
$$\sum_{i=1}^{k}\alpha_i x_i \equiv 0 \pmod{2^{n+1}},$$

故有
$$\sum_{i=1}^{k}\alpha_i x_i \geqslant 2^{n+1}.$$

从而，必有某个 x_j，使

$$x_j\sum_{i=1}^{k}\alpha_i \geqslant 2^{n+1}. \qquad ③$$

由①，②，③得

$$2^{n+1} \leqslant x_j\sum_{i=1}^{k}\alpha_i < x_j \cdot \frac{2^n}{n+1},$$

从而有 $x_j>2(n+1)$，故

$$p_j=2^{n+1}x_j+1>2^{n+1}(2n+2)=2^{n+2}(n+1).$$

例 22 （2004 年国家队集训队测试题）试定出所有满足如下条件的正整数 m：对于 m，存在素数 p，使得对任意整数 n，数 n^n-m 都不是 p 的倍数.

解 $m=1$ 不存在素数 p，使得对任意 n，$p\nmid n-1$(如 $n=p+1$).

下证对 $m\geqslant 2$,均存在相应素数 p,使对一切正整数 n,有 $p\nmid n^m-m$.

设素数 $q|m$,$q^\alpha \| m$. 注意到

$$\frac{m^q-1}{m-1}=1+m+\cdots+m^{q-1}\equiv 1+m(\bmod q^{\alpha+1}).$$

取素数 p,使 $p\left|\frac{m^q-1}{m-1}\right.$,$p\not\equiv 1(\bmod q^{\alpha+1})$，则 $p\left|\frac{m^q-1}{m-1}\right.\cdot(m-1)$,即 $p|m^q-1$, $m^q\equiv 1(\bmod p)$.

若存在整数 n,使 $n^m\equiv m(\bmod p)$,则

$$n^{mq}\equiv m^q\equiv 1(\bmod p),\qquad ①$$

故$(n,p)=1$. 由费马小定理知

$$n^{p-1}\equiv 1(\bmod p).\qquad ②$$

由①②得 $n^{(mq,p-1)}\equiv 1(\bmod p)$.

由 $q^{\alpha+1}\nmid p-1$,结合①知$(mq,p-1)|m$,因此 $n^m\equiv 1(\bmod p)$,从而 $m\equiv n^m\equiv 1(\bmod p)$. 因此

$$0\equiv\frac{m^q-1}{m-1}=1+m+\cdots+m^{q-1}\equiv q(\bmod p),$$

所以 $p=q$. 从而 $p|m$,与 $p|1+m+\cdots+m^{q-1}$矛盾!

所以对任意 n,$p\nmid n^m-m$.

例 23 (CMO-23 试题) 试确定所有同时满足

$$q^{n+2}\equiv 3^{n+2}(\bmod p^n),\ p^{n+2}\equiv 3^{n+2}(\bmod q^n)$$

的三元数组(p,q,n),其中 p,q 为奇素数,n 为大于 1 的整数.

解 易见$(3,3,n)(n=2,3,\cdots)$均为满足要求的数组. 假设(p,q,n)为其他满足要求的一数组,则 $p\neq q,p\neq 3,q\neq 3$. 不妨设 $q>p\geqslant 5$.

如果 $n=2$,则 $q^2|p^4-3^4$,即 $q^2|(p^2-3^2)(p^2+3^2)$. 由于 q 不同时整除 p^2-3^2 和 p^2+3^2,故 $q^2|p^2-3^2$ 或 $q^2|p^2+3^2$. 但 $0<p^2-3^2<q^2$,$\frac{1}{2}(p^2+3^2)<p^2<q^2$,矛盾!

因此 $n\geqslant 3$. 由 $p^n|q^{n+2}-3^{n+2}$,$q^n|p^{n+2}-3^{n+2}$知

$$p^n|p^{n+2}+q^{n+2}-3^{n+2},q^n|p^{n+2}+q^{n+2}-3^{n+2}.$$

又 $p<q$,p,q 为素数,故

$$p^nq^n|p^{n+2}+q^{n+2}-3^{n+2},\qquad ①$$

因此得 $p^nq^n\leqslant p^{n+2}+q^{n+2}-3^{n+2}<2q^{n+2}$,从而 $p^n<2q^2$.

由 $q^n|p^{n+2}-3^{n+2}$及 $p>3$ 知 $q^n\leqslant p^{n+2}-3^{n+2}<p^{n+2}$,从而 $q<p^{1+\frac{2}{n}}$,结合 $p^n<2q^2$ 有 $p^n<2p^{2+\frac{4}{n}}<p^{3+\frac{4}{n}}$. 因此 $n<3+\frac{4}{n}$,故 $n=3$. 这样

$p^3 \mid q^5-3^5, q^3 \mid p^5-3^5$.

且由 $5^5-3^5=2\times11\times131$ 易知 $p>5$. 由 $p^3 \mid q^5-3^5$ 知 $p \mid q^5-3^5$. 由费马小定理知 $p \mid q^{p-1}-3^{p-1}$, 因此 $p \mid q^{(5,p-1)}-3^{(5,p-1)}$.

如果 $(5,p-1)=1$, 则 $p \mid q-3$. 由

$$\frac{q^5-3^5}{q-3}=q^4+q^3\cdot3+q^2\cdot3^2+q\cdot3^3+3^4\equiv5\times3^4 \pmod p,$$

以及 $p>5$ 知 p 不整除 $\frac{q^5-3^5}{q-3}$, 因此 $p^3 \mid q-3$. 由 $q^3 \mid p^5-3^5$ 知

$$q^3\leqslant p^5-3^5<p^5=(p^3)^{\frac{5}{3}}<q^{\frac{5}{3}},\text{矛盾!}$$

所以 $(5,p-1)\neq1$, 即 $5 \mid p-1$, 类似可得 $5 \mid q-1$. 由 $(q,p-3)=1$ (因 $q>p\geqslant7$) 及 $q^3 \mid p^5-3^5$ 知 $q^3 \left| \frac{p^5-3^5}{p-3} \right.$, 从而

$$q^3\leqslant\frac{p^5-3^5}{p-3}=p^4+p^3\cdot3+p^2\cdot3^2+p\cdot3^3+3^4.$$

由 $5 \mid p-1$ 及 $5 \mid q-1$ 知 $p\geqslant11$, $q\geqslant31$. 因此

$$q^3\leqslant p^4\left[1+\frac{3}{p}+\left(\frac{3}{p}\right)^2+\left(\frac{3}{p}\right)^3+\left(\frac{3}{p}\right)^4\right]<p^4\cdot\frac{1}{1-\frac{3}{p}}\leqslant\frac{11}{8}p^4,$$

从而 $p>\left(\frac{8}{11}\right)^{\frac{1}{4}}q^{\frac{3}{4}}$. 因此

$$\frac{p^5+q^5-3^5}{p^3q^3}<\frac{p^2}{q^3}+\frac{q^2}{p^3}<\frac{1}{q}+\left(\frac{11}{8}\right)^{\frac{3}{4}}\frac{1}{31^{\frac{1}{4}}}<1,$$

这与①, 即 $p^3q^3 \mid p^5+q^5-3^5$ 矛盾.

综上, $(3,3,n)(n=2,3,\cdots)$ 即为所有满足要求条件的三元数组.

例 24 (2008 年国家集训队选拔考试题) 数列 $\{x_n\}$ 定义为: $x_1=2$, $x_2=12$, $x_{n+2}=6x_{n+1}-x_n(n=1,2,\cdots)$. 设 p 是一个奇素数, q 是 x_p 的一个素因子. 证明: 若 $q\neq2$, 则 $q\geqslant2p-1$.

证法 1 易知 $x_n=\frac{1}{2\sqrt2}((3+2\sqrt2)^n-(3-2\sqrt2)^n)(n\geqslant1)$. 设正整数 a_n, b_n 由 $(3+2\sqrt2)^n=a_n+b_n\sqrt2$ 定义, 则 $(3-2\sqrt2)^n=a_n-b_n\sqrt2$. 由此易知

$$x_n=b_n, a_n^2-2b_n^2=1(n\geqslant1).$$

设 $q\neq2$, 下面证明 $q\geqslant2p-1$. 由于 $q \mid x_p$, 即 $q \mid b_p$, 从而数列 $\{b_n\}$ 中有被 q 整除的项. 设 d 为最小的正整数, 使 $q \mid b_d$. 我们需要下面的引理.

引理 对正整数 n, 当且仅当 $d \mid n$ 时, 有 $q \mid b_n$.

引理的证明: 对整数 a,b,c,d, 我们用记号 $a+b\sqrt2\equiv c+d\sqrt2 \pmod q$ 表示 $a\equiv c$,

$b\equiv d \pmod q$.

若 $d|n$,设 $n=du$,则 $a_n+b_n\sqrt{2}=(3+2\sqrt{2})^{du}\equiv a_d^u \pmod q$,故 $b_n\equiv 0 \pmod q$.

反过来,若 $q|b_n$,设 $n=du+r,0\leqslant r<d$. 若 $r\geqslant 1$,则由

$$a_n\equiv(3+2\sqrt{2})^n=(3+2\sqrt{2})^{du}\cdot(3+2\sqrt{2})^r\equiv a_d^u(a_r+b_r\sqrt{2}) \pmod q,$$

可知 $a_d^u b_r\equiv 0 \pmod q$. ①

但 $a_d^2-2b_d^2=1$,而 $q|b_d$,故 q 不整除 a_d^2. 因为 q 是素数,所以 q 不整除 a_d,进而 $(q,a_d^u)=1$,故由①知:$q|b_r$,与 d 的定义矛盾! 所以 $r=0$,即 $d|n$. 引理得证.

因为 q 是素数,所以 $C_q^i(1\leqslant i\leqslant q-1)$ 都是 q 的倍数. 由费马小定理知,$3^q\equiv 3 \pmod q$;$2^q\equiv 2 \pmod q$,因 $q\neq 2$,故由此得 $2^{\frac{q-1}{2}}\equiv\pm 1 \pmod q$. 由二项式定理得

$$\begin{aligned}(3+2\sqrt{2})^q&=\sum_{i=0}^{q}C_q^i\cdot 3^{q-i}(2\sqrt{2})^i\equiv 3^q+(2\sqrt{2})^q\\&=3^q+2^q\cdot 2^{\frac{q-1}{2}}\sqrt{2}\equiv 3\pm 2\sqrt{2} \pmod q.\end{aligned} \quad ②$$

因而,类似于②的处理可得

$$(3+2\sqrt{2})^{q^2}\equiv(3\pm 2\sqrt{2})^q\equiv 3+2\sqrt{2} \pmod q. \quad ③$$

由③得:$(a_{q^2-1}+b_{q^2-1}\sqrt{2})(3+2\sqrt{2})\equiv 3+2\sqrt{2} \pmod q$,所以

$$\begin{cases}3a_{q^2-1}+4b_{q^2-1}\equiv 3 \pmod q,\\2a_{q^2-1}+3b_{q^2-1}\equiv 2 \pmod q,\end{cases}$$

进而有 $q|b_{q^2-1}$.

因为 $q|b_p$,故由引理得 $d|p$. 因为 q 是素数,所以 $d=1$ 或 p. 若 $d=1$,则 $q|b_1=2$,这与假设不符,故 $d=p$. 但 $q|b_{q^2-1}$,故由引理知 $d|q^2-1$,即 $p|q^2-1$,从而 $p|q-1$ 或 $p|q+1$. 注意到 $q-1$ 和 $q+1$ 都是偶数,于是有 $q\geqslant 2p-1$,证毕.

证法 2 这一解法,是广西南宁二中学生、获 2007 年中国西部数学奥林匹克第一名的潘锦钊同学给出的.

设 $a_n=\frac{1}{2}x_n$,则 $a_1=1$,$a_2=6$,$a_{n+2}=6a_{n+1}-a_n$.

该数列的特征方程为 $x^2-6x+1=0$,两个特征根为 $\alpha=3+2\sqrt{2}$,$\beta=3-2\sqrt{2}$. 由此易知

$$a_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}\ (n=1,2,\cdots). \quad ④$$

(1) 利用通项公式④,我们证明,对 $m\geqslant 2$,$n\geqslant 1$,有

$$a_{m+n}=a_{m+1}a_n-a_ma_{n-1}. \quad ⑤$$

事实上,⑤的右边为

$$\frac{(\alpha^{m+1}-\beta^{m+1})(\alpha^n-\beta^n)-(\alpha^m-\beta^m)(\alpha^{n-1}-\beta^{n-1})}{(\alpha-\beta)^2}$$

$$=\frac{\alpha^{m+n+1}+\beta^{m+n+1}-(\alpha^{m+n-1}+\beta^{m+n}-1)+\alpha^m\beta^n\left(\frac{1}{\alpha}+\frac{1}{\beta}-\alpha-\beta\right)}{(\alpha-\beta)^2}$$

$$=\frac{\alpha^{m+n+1}+\beta^{m+n+1}-\alpha\beta(\alpha^{m+n-1}+\beta^{m+n-1})}{(\alpha-\beta)^2}$$

$$=\frac{\alpha^{m+n}(\alpha-\beta)-\beta^{m+n}(\alpha-\beta)}{(\alpha-\beta)^2}$$

$=\frac{\alpha^{m+n}-\beta^{m+n}}{\alpha-\beta}=$⑤的左边.

(2) 我们证明，对 m，$n\geqslant1$，有

$(a_m,a_n)=a_{(m,n)}$， ⑥

这里(x,y)表示 x,y 的最大公约数.

为证明⑥,我们先证明：

若 $m|n$,则

$a_m|a_n$,[从而$(a_m,a_n)=a_{(m,n)}$.] ⑦

不妨设 $m\geqslant2$,并设 $n=mk$,k 为正整数. 当 $k=1$ 时⑦显然成立. 设 $a_m|a_{mk}$,则由⑤知,

$a_{m(k+1)}=a_{mk+1}a_m-a_{mk}a_{m-1}$,

是 a_m 的倍数,故由归纳法知 $a_m|a_{mk}$对所有 k 成立,从而⑦得证.

其次证明:对 $n\geqslant1$,有

$(a_n,a_{n+1})=1$. ⑧

当 $n=1$ 时,⑧显然成立. 设⑧在 $n=k$ 时成立,则有

$(a_{k+1},a_{k+2})=(a_{k+1},6a_{k+1}-a_k)=(a_{k+1},a_{k-1})=1$,

即⑧在 $n=k+1$ 时也成立,故由归纳法知⑧成立.

现在我们证明⑥. 可设 $m-n>1$,且 $n>1$,否则⑥可由⑦或⑧推出来. 由⑤及⑧可得

$(a_m,a_n)=(a_{m-n+1}a_n-a_{m-n}a_{n-1},a_n)=(a_{m-n}a_{n-1},a_n)=(a_{m-n},a_n)$. ⑨

由⑨,并利用求(m,n)的欧几里得算法,以及⑦,⑧中的结果,便不难推出⑥中说的等式(细节请读者自己完成).

(3) 下面证明:

对任意奇素数 p，有

$p\mid a_{\frac{p-1}{2}}a_{\frac{p+1}{2}}$. ⑩

事实上，由④得

$$a_{\frac{p-1}{2}}a_{\frac{p+1}{2}}=\frac{(\alpha^{\frac{p-1}{2}}-\beta^{\frac{p-1}{2}})(\alpha^{\frac{p+1}{2}}-\beta^{\frac{p+1}{2}})}{(\alpha-\beta)^2}=\frac{\alpha^p+\beta^p-(\alpha+\beta)}{(\alpha-\beta)^2}$$

$$=\frac{(3+2\sqrt{2})^p+(3-2\sqrt{2})^p-6}{32}.$$

由二项式定理可得

$$(3+2\sqrt{2})^p+(3-2\sqrt{2})^p=2(C_p^0 3^p+C_p^2 3^{p-2}(2\sqrt{2})^2+C_p^4 3^{p-4}(2\sqrt{2})^4+\cdots)$$

$$\equiv 2\cdot 3^p\equiv 2\times 3\equiv 6 \pmod p.$$

(我们应用了 $p\mid C_p^i$ 对 $1\leqslant i\leqslant p-1$,及费马小定理.)

故 $32a_{\frac{p-1}{2}}a_{\frac{p+1}{2}}\equiv 6-6\equiv 0 \pmod p$.

因 p 是奇素数,故由上式即得⑩.

回到原问题. 设 $q\mid x_p$, $q\neq 2$,则 $q\mid a_p$. 若 $q<2p-1$,则 $\left(p,\frac{q-1}{2}\right)=\left(p,\frac{q+1}{2}\right)=1$,从而由⑥推出 a_p 与 $a_{\frac{q-1}{2}}$ 及 $a_{\frac{q+1}{2}}$ 都互素(注意 $a_1=1$),故 $(a_p,a_{\frac{q-1}{2}}a_{\frac{q+1}{2}})=1$.

但⑩表明 $q\mid a_{\frac{q-1}{2}}a_{\frac{q+1}{2}}$,又 $q\mid a_p$,从而 $q\mid(a_p,a_{\frac{q-1}{2}}a_{\frac{q+1}{2}})$,矛盾. 故 $q\geqslant 2p-1$. 证毕.

注 前一种解法中的引理,是⑥的一个推论.

【模拟实战】

1. (1988 年第 51 届莫斯科数学奥林匹克题)证明当素数 $p\geqslant 7$ 时,p^4-1 能被 240 整除.
2. (IMO-26 预选题)设 $k\geqslant 2$,n_1,n_2,…,n_k 为自然数,满足 $n_2\mid 2^{n_1}-1$,$n_3\mid 2^{n_2}-1$,…,$n_k\mid 2^{n_{k-1}}-1$,$n_1\mid 2^{n_k}-1$. 证明 $n_1=n_2=\cdots=n_k=1$.
3. (第 18 届韩国数学奥林匹克题)求所有的整数 m 和 n,使得 $mn\mid(3^m+1)$,$mn\mid(3^n+1)$.
4. (第 36 届加拿大数学奥林匹克题)设 p 是奇素数,证明 $\sum\limits_{k=1}^{p-1}k^{2p-1}\equiv\frac{p(p+1)}{2} \pmod{p^2}$.
5. (第 54 届波兰数学奥林匹克题)求所有整系数多项式 W,满足:对于每个正整数 n,整数 2^n-1 可以被 $W(n)$ 整除.
6. (第 36 届奥地利数学奥林匹克题)设 f 是定义在$\{0,1,\cdots,2005\}$上的函数,取值于非负整数,对任意满足定义域的变量 x,都有 $f(2x+1)=f(2x)$,$f(3x+1)=f(3x)$,$f(5x+1)=f(5x)$. 问:这个函数最多能取到多少个函数值?
7. (IMO-32 预选题)在 $n!$ 的十进制表示中,从个位数算起第一个非零数字记为 a_n,问是否存在自然数 N,使得 a_{N+1},a_{N+2},a_{N+3},…是周期数列?
8. (1972 年第 33 届美国普特南数学竞赛)设 n 为大于 1 的整数,求证 2^n-1 不能被 n 整除.

9. (IMO-29 预选题) 设 $g(n)$ 定义如下: $g(1)=0, g(2)=1, g(n+2)=g(n)+g(n+1)+1(n\geqslant 1)$. 证明若 $n>5$ 为素数, 则 $n\mid g(n)(g(n)+1)$.
10. (IMO-13 试题) 试证对于数列 $\{2^n-3\}, n=2,3,4,\cdots$, 至少有一个无穷子列存在, 其中的项两两互素.
11. (2007 年爱沙尼亚国家队选拔考试题) 设 n 为大于或等于 2 的自然数. 证明: 若存在正整数 b, 使得 $\frac{b^n-1}{b-1}$ 是某个素数的若干次幂, 则 n 必为素数.
12. (IMO-31 预选题) 试求所有的自然数 n, 使得由 $n-1$ 个数码 1 和 1 个数码 7 构成的每一个十进制表示的自然数, 都是素数.
13. (CMO-14 试题) 设 m 是给定的整数, 求证: 存在整数 a, b 和 k, 其中 a, b 均不能被 2 整除, $k>0$, 使得 $2m=a^{19}+b^{99}+k\cdot 2^{1999}$.
14. 已知 m, n 为正整数并且 $(m,n)=1$. 设 $\{a_1,a_2,\cdots,a_s\}$, $\{b_1,b_2,\cdots,b_t\}$ 分别是模 m 与模 n 的缩系. 证明: $S=\{mb_j+na_i \mid 1\leqslant i\leqslant s, 1\leqslant j\leqslant t\}$ 是模 mn 的缩系.
15. 已知正整数 $k\geqslant 2$, p_1, p_2, $\cdots$, p_k 为奇素数, 且 $(a, p_1p_2\cdots p_k)=1$. 证明: $a^{(p_1-1)\cdots(p_k-1)}-1$ 有不同于 p_1, p_2, $\cdots$, p_k 的奇素因数.
16. (IMO-34 预选题) 对正整数 n, 如果对任意 $a\in \mathbf{N}^+$, 只要 $n\mid a^n-1$, 就有 $n^2\mid a^n-1$, 则称 n 具有性质 P.
    (1) 求证: 每个素数都具有性质 P;
    (2) 求证: 存在无穷多个合数具有性质 P.
17. 设 p 为奇素数, a, $n\in \mathbf{N}^+$, 并且 a^p-1 是 p^n 的倍数. 证明: $a-1$ 是 p^{n-1} 的倍数. 又问: 当 $p=2$ 时, 命题是否依然成立?
18. (IMO-44 试题) 设 p 是素数. 证明: 存在一个素数 q, 使得对任意整数 n, 数 n^p-p 不是 q 的倍数.
19. (IMO-40 试题) 确定所有的正整数对 (n,p), 满足: p 是一个素数, $n\leqslant 2p$, 且 $(p-1)^n+1$ 能够被 n^{p-1} 整除.

第十三章　中国剩余定理

【基础知识】

定义 1　设 $f_j(x)$ 为整系数多项式($1\leqslant j\leqslant k$)，我们把含有 x 的一组同余式 $f_j(x)\equiv 0 \pmod{m_j}$($1\leqslant j\leqslant k$)称为同余方程组. 特别地，当 $f_j(x)$ 均为 x 的一次整系数多项式时，该同余方程组称为一次同余方程组. 若整数 c 同时满足

$$f_j(c)\equiv 0 \pmod{m_j},\ 1\leqslant j\leqslant k,$$

则剩余数 $M_c=\{x\mid x\in\mathbf{Z}, x\equiv c \bmod m\}$(其中 $m=[m_1,m_2,\cdots,m_k]$)称为同余方程组的一个解，写作 $x\equiv c \pmod m$.

中国剩余定理　设 m_1，m_2，…，m_k 是两两互素的正整数，那么，对于任意整数 a_1，a_2，…，a_k，一次同余方程组

$$\begin{cases} x\equiv a_1 \pmod{m_1}, \\ x\equiv a_2 \pmod{m_2}, \\ \cdots \\ x\equiv a_k \pmod{m_k} \end{cases}$$

必有解，且解可写为

$$x\equiv M_1N_1a_1+M_2N_2a_2+\cdots+M_kN_ka_k \pmod m.$$

这里 $m=m_1m_2\cdots m_k$，$M_i=\dfrac{m}{m_i}$($1\leqslant i\leqslant k$)，以及 N_j 满足 $M_jN_j\equiv 1 \pmod{m_j}$，$1\leqslant j\leqslant k$(即 N_j 为 M_j 对模 m_j 的逆).

(注：中国剩余定理又叫孙子定理.)

证明　分为两个步骤来证明定理.

(1) $x\equiv M_1N_1a_1+M_2N_2a_2+\cdots+M_kN_ka_k \pmod m$ 是同余方程组 $x\equiv a_j \pmod{m_j}$ ($1\leqslant j\leqslant k$)的解.

事实上，设 $x\equiv M_1N_1a_1+M_2N_2a_2+\cdots+M_kN_ka_k \pmod m$，$x\in\mathbf{Z}$. 由于 $m_j\mid M_i$($i\neq j$)以及 $m_j\mid m$，故对 $1\leqslant j\leqslant k$ 有 $x-M_jN_ja_j \pmod{m_j}$，而 $M_jN_j\equiv 1 \pmod{m_j}$，所以 $x\equiv a_j \pmod{m_j}$.

从而 x 的确是同余方程组的解.

(2) 设整数 x,y 同时满足方程组，即 $x\equiv a_j \pmod{m_j}(1\leqslant j\leqslant k)$，$y\equiv a_j \pmod{m_j}$ $(1\leqslant j\leqslant k)$，则有 $x\equiv y \pmod{m}$.

事实上，由 $x\equiv y\equiv a_j \pmod{m_j}$ 可知 $m_j \mid (x-y)(1\leqslant j\leqslant k)$.

又 $m_1,m_2,\cdots,m_k$ 两两互素，则

$m_1m_2\cdots m_k \mid (x-y)$，亦即 $m\mid(x-y)$.

故 $x\equiv y \pmod{m}$.

综合 (1)，(2) 可知，定理得证.

定理 1（拉格朗日定理） 设 p 是素数，n 是非负整数，多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是一个模 p 为 n 次的整系数多项式（即 $p\nmid a_n$），则同余方程

$$f(x)\equiv 0 \pmod{p} \tag{*}$$

至多有 n 个解(在模 p 的意义下).

证明 我们对 n 用归纳法.

当 $n=0$ 时，$f(x)=a_0$，因为 $p\nmid a_0$，故同余方程(*)无解，命题成立.

设当 $n=l$ 时命题成立，则当 $n=l+1$ 时，若命题不成立，即同余方程(*)至少有 $l+2$ 个解，设为 $x\equiv c_1,c_2,\cdots,c_{l+2} \pmod{p}$. ①

我们考虑多项式

$$\begin{aligned}f(x)-f(c_1)&=a_{l+1}(x^{l+1}-c_1^{l+1})+a_l(x^l-c_1^l)+\cdots+a_1(x-c_1)\\&=(x-c_1)(a_{l+1}x^l+\cdots)=(x-c_1)h(x),\end{aligned} \quad ②$$

其中 $h(x)$ 是 l 次多项式并且首项系数 a_{l+1} 满足 $p\mid a_{l+1}$，从而由归纳假设知 l 次同余方程

$$h(x)\equiv 0 \pmod{p} \quad ③$$

至多有 l 个解，但由①，②可知同余方程③至少有 $l+1$ 个解

$x\equiv c_2,c_3,\cdots,c_{l+2} \pmod{p}$，

矛盾！故当 $n=l+1$ 时命题成立.

综上所述，命题得证.

定义 2 假设 a，m 为两个互素的正整数，则存在最小的正整数 l，使 $a^l\equiv 1 \pmod{m}$[由欧拉定理可知这样的 l 存在且不超过 $\varphi(m)$]，则称 l 为 a 对模 m 的阶.

定理 2 若 l 为 a 对模 m 的阶，s 为某一正整数，满足 $a^s\equiv 1 \pmod{m}$，则 s 必为 l 的倍数.

证明 由阶的定义可知 $s\geqslant l$，故可设 $s=kl+l_0$，这里 $k\in \mathbf{Z}^+$，而 $0\leqslant l_0<l$.

用反证法证明定理 2，反设 $l\nmid s$，则 $l_0\geqslant 1$.

从而 $a^s=a^{kl+l_0}\equiv (a^l)^k a^{l_0} \pmod{m}$.

由于 $a^s=1 \pmod{m}$，$a^l\equiv 1 \pmod{m}$，所以

$a^{l_0}\equiv 1 \pmod{m}$.

于是我们找到了一个比 l 小的正整数 l_0，满足 $a^{l_0}\equiv 1 \pmod{m}$，这与 l 为 a 对模 m 的阶的取法及阶的定义相矛盾，从而反设不成立，定理 2 得证.

以上介绍的都是一些知识、方法，经常在解决数论问题中起着突破难点的作用. 另外有一些小的技巧则是在思考、解决问题中起着排除情况、辅助分析等作用的，有时甚至起到意想不到的效果. 如

定理 3

$$n^2\begin{cases}\equiv 1 \pmod{8}(n\text{ 为奇数时});\\ \equiv 0 \pmod{4}(n\text{ 为偶数时}).\end{cases}$$

$$n^2\begin{cases}\equiv 0 \pmod{9}(3\mid n\text{ 时});\\ \equiv 0 \pmod{3}(3\nmid n\text{ 时}).\end{cases}$$

【典型例题与基本方法】

例 1 解同余方程组 $\begin{cases}x\equiv 1 \pmod{7},\\ x\equiv 1 \pmod{8},\\ x\equiv 3 \pmod{9}.\end{cases}$

解 由于 7，8，9 两两互素，则知同余方程组有解.

$M=7\cdot 8\cdot 9=504, M_1=\frac{504}{7}=72, M_2=\frac{504}{8}=63, M_3=\frac{504}{9}=56$. 从而

$$M_1'\equiv\frac{1}{72}\equiv\frac{1}{7\cdot 10+2}\equiv\frac{1}{2}\equiv\frac{4}{8}\equiv\frac{4}{7+1}\equiv 4 \pmod{7},$$

$$M_2'\equiv\frac{1}{63}\equiv\frac{1}{64-1}\equiv\frac{1}{-1}\equiv -1\equiv 7 \pmod{8},$$

$$M_3'\equiv\frac{1}{56}\equiv\frac{1}{6\cdot 9+2}\equiv\frac{1}{2}\equiv\frac{5}{10}\equiv\frac{5}{9+1}\equiv 5 \pmod{9}.$$

故 $x\equiv 4\cdot 72\cdot 1+7\cdot 63\cdot 1+5\cdot 56\cdot 3\equiv 57 \pmod{504}$ 为所求.

例 2 今有数不知总，以 5 累减之无剩，以 715 累减之剩 10，以 247 累减之剩 140，以 391 累减之剩 245，以 187 累减之剩 109. 问总数若干?

解 设总数为 x，则有同余式组 $\begin{cases}x\equiv 0 \pmod{5},\\ x\equiv 10 \pmod{715},\\ x\equiv 140 \pmod{247},\\ x\equiv 245 \pmod{391},\\ x\equiv 109 \pmod{187}.\end{cases}$

因 5，715，247，391，187 不两两互素，但有

$(5,715)=5|(10-0)$，$(715,247)=13|(140-10)$，

$(715,187)=11|(109-10)$，$(391,187)=17|(245-109)$.

从而$[5,715,247,391,187]=[5,143,19,23,17]$，且 5，143，19，23，17 两两互素，

故原同余方式组的等价同余组有解. 等价的同余式组为$\begin{cases}x\equiv 0 \pmod 5,\\ x\equiv 10 \pmod{143},\\ x\equiv 140\equiv 7 \pmod{19},\\ x\equiv 245\equiv 15 \pmod{23},\\ x\equiv 109\equiv 7 \pmod{17}.\end{cases}$

此时 $M=5\cdot 143\cdot 19\cdot 23\cdot 17=5311735$.

$M_1=\frac{M}{5}, M_2=\frac{M}{143}, M_3=\frac{M}{19}, M_4=\frac{M}{23}, M_5=\frac{M}{17}$.

于是$M_1'\equiv 3 \pmod 5$，$M_2'\equiv 49 \pmod{143}$，$M_3'\equiv -1 \pmod{19}$，

$M_4'\equiv 1 \pmod{23}$，$M_5'\equiv -7 \pmod{17}$.

故 $x\equiv 3\cdot 1062347\cdot 0+49\cdot 37145\cdot 10+(-1)\cdot 279565\cdot 7+1\cdot 230945\cdot 15+(-7)\cdot 312455\cdot 7\equiv 10020 \pmod{5311735}$.

此即为所求.

例 3 （2007 年国家集训队测试题）是否存在无穷多个正整数 k 使得 $k\cdot 2^n+1$ 对每个正整数 n 都是合数?

解法 1 设 $i>j$，显然

$2^{2^j}+1 \mid 2^{2^i}-1$，

所以，$\gcd(2^{2^i}+1,2^{2^j}+1)|2$ 且两数皆是奇数. 因此对于 $i\geqslant 0$，费马数 $f_i=2^{2^i}+1$ 两两互素.

令 p_i 是 $2^{2^i}+1$ 的一个素因子，则对每个具有形式 $2^i\cdot q$，q 为奇数的 n，成立

$2^n=2^{2^i\cdot q}\equiv -1 \pmod{p_i}$，

进而对 $k\equiv 1 \pmod{p_i}$，我们有 $p_i|2^n\cdot k+1$.

而对每个具有形式 $2^i\cdot q$，q 为偶数的 n，成立

$2^n=2^{2^i\cdot q}\equiv 1 \pmod{p_i}$，

进而对 $k\equiv 1 \pmod{p_i}$，我们有 $p_i|2^n\cdot k+1$.

对 $i=0, 1, 2, 3, 4$，令 p_i 是 $2^{2^i}+1$ 的素因子，p，q 是 $2^{32}+1$ 的两个不同的素因子（即 641 和 6700417）. 根据中国剩余定理，我们可选取 k 使得对 $i=0, 1, 2, 3, 4$，$k\equiv 1 \pmod{p_i}$，$k\equiv 1 \pmod p$ 以及 $k\equiv -1 \pmod q$.

令 i 是满足 $2^i|n$ 的最大整数，则由上可知当 $i=5$ 时 $p|2^n\cdot k+1$；当 $i<5$ 时 $p_i|2^n\cdot k+1$；对 $i>5$，因为 $k\equiv -1 \pmod q$，所以 $q|2^n\cdot k+1$. 因此如果我们选取充分大的

k，则 $2^n \cdot k+1$ 对所有 $n \geqslant 0$ 都是合数.

解法 2 注意到

$2^2 \equiv 1 \pmod 3$，$2^4 \equiv 1 \pmod 5$，$2^3 \equiv 1 \pmod 7$，

$2^{12} \equiv 1 \pmod{13}$，$2^8 \equiv 1 \pmod{17}$，$2^{24} \equiv 1 \pmod{241}$.

利用中国剩余定理，我们可选取 k 使得

$2k \equiv -1 \pmod 3$，$2^4 \cdot k \equiv -1 \pmod 5$，$2^2 \cdot k \equiv -1 \pmod 7$，

$2^6 \cdot k \equiv -1 \pmod{13}$，$2^{10} \cdot k \equiv -1 \pmod{17}$，$2^{22} \cdot k \equiv -1 \pmod{241}$.

对这样的正整数 k，我们有以下的表：

n	1	2	3	4	5	6	7	8
p	3	7，17	3	5	3，7	13	3	5，7
n	9	10	11	12	13	14	15	16
p	3	17	3，7	5	3	7	3	5
n	17	18	19	20	21	22	23	24
p	3，7	13，17	3	5，7	3	24	3，7	5

（这里 n 的值取为模 24，p 表示相应的数 $2^n \cdot k+1$ 的素因子.）

例 4 （2004 年西班牙数学竞赛题）设 n 和 k 是正整数，其中 n 是奇数或 n 和 k 都是偶数. 证明：存在整数 a，b，使得

$(a,n)=1$，$(b,n)=1$，$k=a+b$.

证明 （1）若 n 是奇素数或奇素数的幂，设 $n=p^a$.

因为 $k=1+(k-1)$，$k=2+(k-2)$，$(1,p^a)=(2,p^a)=1$，$k-1$ 和 $k-2$ 中一定有一个与 p 互素，从而，也与 p^a 互素.

所以，两式中一定有一个满足条件.

因此，n 是奇素数或奇素数的幂时命题成立.

（2）若 n 是奇数，设 $n=p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$，其中 p_1，p_2，…，p_m 是奇素数.

由（1），对 $i=1$，2，…，m，存在整数 a_i，b_i 满足

$k=a_i+b_i$，$(a_i,p_i^{a_i})=1$，$(b_i,p_i^{a_i})=1$.

考虑同余方程组

$x \equiv a_i \pmod{p_i^{a_i}}$，$i=1,2,\cdots,m$.

由中国剩余定理，存在整数 a' 使得

$a' \equiv a_i \pmod{p_i^{a_i}}$，$i=1,2,\cdots,m$.

于是，$(a',p_i^{a_i})=(a_i,p_i^{a_i})=1$.

故 $(a',n)=1$.

同理，存在整数 b' 使得

$b'\equiv b_i \pmod{p_i^{\alpha_i}}$，$i=1,2,\cdots,m$，且 $(b',n)=1$.

由于 $k=a_i+b_i\equiv a'+b' \pmod{p_i^{\alpha_i}}$，$i=1,2,\cdots,m$，由中国剩余定理得

$k\equiv a'+b' \pmod n$.

设 $k=a'+b'+tn$，又设 $a=a'$，$b=b'+tn$，则

$(a,n)=1$，$(b,n)=(b',n)=1$，$k=a+b$.

因此，n 是奇数时命题成立.

(3) 若 n 是偶数，则 k 也是偶数.

设 $n=2^{\beta}n_0$，其中 n_0 是奇数. 由 (2)，存在整数 a_0，b_0，使得

$(a_0,n_0)=1$，$(b_0,n_0)=1$，$a_0+b_0=k$.

若 a_0，b_0 都是奇数，则 $(a_0,n)=1$，$(b_0,n)=1$，命题成立.

若 a_0，b_0 都是偶数，设 $a=a_0+n_0$，$b=b_0-n_0$，则 a，b 都是奇数. 所以，

$(a,n)=1$，$(b,n)=1$，$a+b=k$.

因此，n 是偶数时命题成立.

【解题思维策略分析】

1. 善于运用中国剩余定理处理问题

例 5 （第 34 届俄罗斯数学奥林匹克题）找出所有满足如下条件的整数 $n(n>1)$：存在不全相等的正整数 b_1，b_2，…，b_n，使得对任意给定的正整数 k，都存在正整数 a，$b(a,\ b>1)$ 满足 $\prod\limits_{i=1}^{n}(b_i+k)=a^b$.

解 $n>1$ 满足条件当且仅当 n 是合数.

当 $n=rs(r>1,s>1)$ 为合数时，令

$b_1=b_2=\cdots=b_r=1$，

$b_{r+1}=b_{r+2}=\cdots=b_n=2$.

则对任意正整数 k，$(b_1+k)(b_2+k)\cdots(b_n+k)$ 是一个正整数的 r 次幂.

当 n 为一个素数时，设存在不全相等的正整数 b_1，b_2，…，b_n，使得对任意给定的正整数 k，都存在正整数 a，b (a，$b>1$) 满足

$(b_1+k)(b_2+k)\cdots(b_n+k)=a^b$.

不妨设 $b_1,b_2,\cdots,b_l(l>1)$ 两两不同，而 $b_{l+1},b_{l+2},\cdots,b_n$ 中的每一个都等于 b_1，$b_2,\cdots,b_l$ 之一. 设 $b_1,b_2,\cdots,b_n$ 中有 s_i 个等于 $b_i(1\leqslant i\leqslant l)$，$s_1+s_2+\cdots+s_l=n$.

我们将利用如下的中国剩余定理：对任意的两两互素的正整数 a_1，a_2，…，a_l 及非负整数 r_1，r_2，…，r_l，$r_i<a_i$ ($1\leqslant i\leqslant l$)，都存在正整数 m，满足

$m \equiv r_i \pmod{a_i}(i=1,2,\cdots,l)$.

令 p_1, p_2, $\cdots$, $p_l > \max\{b_1, b_2, \cdots, b_l\}$ 是 l 个不同的素数.

对 $a_i = p_i^2$, $r_i = p_i - b_i(1 \leqslant i \leqslant l)$应用中国剩余定理得,存在正整数 m,使得

$b_i + m \equiv p_i \pmod{p_i^2}$.

从而,$m+b_i$ 是 p_i 的倍数,但不是 p_i^2 的倍数.

另外,对 $j \neq i(1 \leqslant j \leqslant l)$,由于$|b_i - b_j| < p_i$,$b_j + m$ 不是 p_i 的倍数,因此,

$a^b = (b_1+m)(b_2+m)\cdots(b_n+m)$是 $p_i^{s_i}$ 的倍数,但不是 $p_i^{s_i+1}$的倍数.

故 $b | s_i(1 \leqslant i \leqslant l)$.

注意到 $n = s_1 + s_2 + \cdots + s_l$,有 $b | n$.

由于 $l > 1$,得 $b < n$.

又 n 为素数,得 $b=1$. 矛盾.

例 6 (IMO-39 预选题) 确定所有正整数 n,存在一个整数 m,使得 $2^n - 1$ 是 m^2+9 的一个因数.

解 我们证明所求的 $n=2^k$,k 为非负整数.

首先证明 n 没有奇因数.

假设 n 有奇因数 s,则 2^s-1 是 $2^n - 1 = (2^s)^{\frac{n}{s}} - 1$ 的一个因数.

如果 $2^n - 1$ 是 m^2+9 的因数,则 2^s-1 也是 m^2+9 的因数.

设 $s = 2t+1$,则 $2^s - 1 = 2 \cdot 4^t - 1 = 2(3+1)^t - 1$,于是 $3 \nmid 2^s - 1$,则

$2^s - 1 \equiv -1 \pmod 4$.

这样 2^s-1 必有一个素约数 $p>3$,满足

$p \equiv -1 \pmod 4$.

从而由 p 是 m^2+9 的因数可知

$m^2 \equiv -9 \pmod p$,$m^{p-1} \equiv -9^{\frac{p-1}{2}} = -3^{p-1} \pmod p$.

若$(m,p)=1$,由 $p>3$,则由上式有 $1 \equiv -1 \pmod p$.

若 $p | m$,则由上式有 $0 \equiv -1 \pmod p$.

上两情况都产生矛盾,故 n 没有奇因子.

下面再证明:对 $n=2^k$,一定存在整数 m,使 2^n-1 是 m^2+9 的一个因数.

对 $2^n - 1 = 2^{2^k} - 1$ 进行分解:

$$\begin{aligned}2^n - 1 &= 2^{2^k} - 1 = (2^{2^{k-1}}+1)(2^{2^{k-1}}-1) = (2^{2^{k-1}}+1)(2^{2^{k-2}}+1)(2^{2^{k-2}}-1)\\&= \cdots = (2^{2^{k-1}}+1)(2^{2^{k-2}}+1)\cdots(2^{2^1}+1)(2^2+1)(2+1).\end{aligned}$$

从而,同余方程 $x^2 \equiv -1 \pmod{2^{2^k}+1}$有解

$x \equiv 2^{2^{k-1}} \pmod{2^{2^k}+1}$.

而 $j>i$ 时,$(2^{2^i}+1, 2^{2^j}+1) = (2^{2^{i+1}}-1, 2^{2^j}+1) = \cdots = (2, 2^{2^j}+1) = 1$.

根据中国剩余定理，同余方程组 $x\equiv 2^{2^{h-1}}(\bmod\ 2^{2^h}+1)$，$h=1,2,\cdots,k-1$ 有解 x_0.

令 $m-3x_0$，则 $m^2+9=9(x_0^2+1)$ 被 $2^{2^k}-1$ 整除，即被 2^m-1 整除.

例 7 （CMO－23 试题）设 A 是正整数集的无限子集，$n>1$ 是给定的整数. 已知：对任意一个不整除 n 的素数 p，集合 A 中均有无穷多个元素不被 p 整除.

证明：对任意整数 $m>1$，$(m,n)=1$；集合 A 中均存在有限个不同元素，其和 S 满足 $S\equiv 1(\bmod\ m)$，且 $S\equiv 0(\bmod\ n)$.

证法 1 设 $p^{\alpha}\parallel m$，$\alpha\geqslant 1$，则集合 A 中有一个无穷子集 A_1，其中的元素都不被 p 整除. 由抽屉原理知，集合 A_1 有一个无穷子集 A_2，其中的元素都 $\equiv a(\bmod\ mn)$，a 是一个不被 p 整除的数.

因 $(m,n)=1$，故 $\left(p^{\alpha},\frac{mn}{p^{\alpha}}\right)=1$. 由中国剩余定理，同余方程组

$$\begin{cases}x\equiv a^{-1}(\bmod\ p^{\alpha}),\\ x\equiv 0\left(\bmod\ \frac{mn}{p^{\alpha}}\right)\end{cases} \quad ①$$

有无穷多个整数解. 任取其中一个正整数解 x，并记 B_p 是 A_2 中前 x 项的集合，则 B_p 中的元素之和 $S_p\equiv ax(\bmod\ mn)$，再由①可知

$$S_p\equiv ax\equiv 1(\bmod\ p^{\alpha}),S_p\equiv 0\left(\bmod\ \frac{mn}{p^{\alpha}}\right).$$

设 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，并设对每个 $p_i(1\leqslant i\leqslant k-1)$ 已选出了 A 的有限子集 B_{p_i}，其中 $B_{p_i}\subset A\setminus B_{p_1}\cup\cdots\cup B_{p_{i-1}}$，使得 B_{p_i} 中的元素和 S_{p_i} 满足

$$S_{p_i}\equiv 1(\bmod\ p_i^{\alpha_i}),S_{p_i}\equiv 0\left(\bmod\ \frac{mn}{p_i^{\alpha_i}}\right). \quad ②$$

考虑集合 $B=\bigcup\limits_{i=1}^{k}B_{p_i}$，则 B 的元素和 $S=\sum\limits_{i=1}^{k}S_{p_i}$. 根据②，我们有

$S\equiv 1\ (\bmod\ p_i^{\alpha_i})\ (1\leqslant i\leqslant k)$，且 $S\equiv 0\ (\bmod\ n)$.

所以 B 即满足题目要求.

证法 2 考虑 A 中的数除以 mn 的余数，设出现无穷多次的余数依次为 a_1，a_2，$\cdots$，a_k.

首先证明

$$(a_1,a_2,\cdots,a_k,m)=1. \quad ③$$

用反证法. 设有某个素数 $p\mid(a_1,a_2,\cdots,a_k,m)$，则由 $(m,n)=1$ 知 p 不整除 n. 又根据 $a_1,a_2,\cdots,a_k$ 的定义，A 中只有有限个数不是 p 的倍数，这与题设矛盾.

于是③获证. 从而存在正整数 x_1，x_2，$\cdots$，x_k，y，使得

$$a_1x_1+a_2x_2+\cdots+a_kx_k-ym=1.$$

再取合适的正整数 r 使得 $rn\equiv 1(\bmod m)$，则

$a_1(rnx_1)+a_2(rnx_2)+\cdots+a_k(rnx_k)=rn+rmny$.

于是从 A 中依次取出 rnx_i 个模 mn 的余数为 a_i 的数（$i=1$，2，$\cdots$，k）即满足题目要求.

例 8 （IMO－33 预选题）是否存在具有如下性质的集合 M：

(1) 集合 M 由 1992 个自然数所构成；

(2) M 中的任何元素以及其中任意个元素之和都具有 m^k 的形式（$m,k\in\mathbf{N},k\geq 2$）？

解法 1 我们考察更一般的问题：

对于任何正整数 n，都存在由 n 个自然数所构成的集合 M_n 满足条件 (2).

下面通过对 n 归纳来证明这个命题.

命题对于 $n=2$ 是成立的.

例如可取 $M_2=\{9,16\}$.

假设对于 $k\geq 2$，集合 $M_k=\{a_1,a_2,\cdots,a_k\}$ 满足条件 (2). 并假定其中元素的所有 2^k-1 个不同的和数可以分别地表示为

$S_1^{\alpha_1}$，$S_2^{\alpha_2}$，$\cdots$，$S_{2^k-1}^{\alpha_{2^k-1}}$，其中 $\alpha_i\geq 2(i=1,2,\cdots,2^k-1)$.

设 α_1，α_2，$\cdots$，α_{2^k-1} 的最小公倍数是 m.

取 2^k-1 个不同的素数 p_i （$i=1$，2，$\cdots$，2^k-1），使得 $(m,p_i)=1$，$i=1$，2，$\cdots$，2^k-1（因为素数有无穷多个，这一点是可以做得到的）.

令 $c_i=\prod\limits_{\substack{j=1\\ j\neq i}}^{2^k-1}p_j,i=1,2,\cdots,2^k-1$,

则有 $(mc_i,p_i)=1$.

再令 $mc_ik_j+1=q_jp_i+r_j,j=1,2,\cdots,p_i,0\leq r_j<p_i$.

则所有的这些 r_j 各不相同.

事实上，如果这些 r_j 有些相同，例如

$r_{j_1}=r_{j_2},1\leq j_1<j_2\leq p_i$.

则有 $p_i\mid[(mc_ik_2+1)-(mc_ik_1+1)]$，即 $p_i\mid mc_i(k_2-k_1)$.

由 $(mc_i,p_i)=1$ 及 $|k_2-k_1|<p_i$ 可知，这是不可能的.

于是，所有的 p_i 个 r_j 各不相同，因此，在这些 r_j 中必有一个为零，因而相应的数可被 p_i 整除，设该数为 mc_ik_i+1.

另一方面，由中国剩余定理（即孙子定理）可知，存在自然数 x，使得

$$\begin{cases} x\equiv k_1 \pmod{p_1}, \\ x\equiv k_2 \pmod{p_2}, \\ \cdots\cdots \\ x\equiv k_{2^k-1} \pmod{p_{2^k-1}}. \end{cases}$$

于是，由 $p_i \mid mc_ik_i+1$ 得

$p_i \mid mc_ix+1, i=1,2,\cdots,2^k-1.$

令　$b=\prod\limits_{i=1}^{2^k-1}(S_i'+1)^{mc_ix}.$

并以 M_k 为基础构造集合 M_{k+1}：

$M_{k+1}=\{a_1b, a_2b, \cdots, a_kb, b\}.$

下面再证明 M_{k+1} 满足条件（2）.

考虑两种情形：

（i）b 不参与求和.

这样的和均具有形式 $S_i'b$.

由于 b 是一个自然数的 m 次方幂，而 m 是 a_1，a_2，…，a_{2^k-1} 的最小公倍数，所以 b 是某个自然数的 a_i（$i=1$，2，…，2^k-1）次方幂．因此，所有这样的和数均符合要求，即满足条件（2）.

（ii）b 参与求和.

此时各和数均具有形式 $(S_i'+1)b$.

该数的因数具有下列形式：

$(S_i'+1)^{mc_ix+1}$，对于 i；

$(S_j'+1)^{mc_jx}$，对于所有 $j\neq i$.

但是，由于 $p_i \mid mc_ix+1$，$p_i \mid mc_jx$，$j\neq i$.

因此，这种和数是自然数的 p_i 次方幂.

因而，命题对 $n=k+1$ 成立.

于是，对所有大于或等于 2 的自然数 n，都存在由 n 个自然数所构成的集合 M_n，满足条件（2）.

解法 2　本题的解答蕴涵在如下的引理中.

引理　对于每个自然数 n，都存在自然数 d，使得数列 d，$2d$，…，nd 中的各数都具有形式

$m^k (m, k\in \mathbf{N}, k\geqslant 2).$

下面用数学归纳法证明这个引理.

$n=1$ 时，引理显然.

这时可取 $d-1$，于是

$d=m^k,(m=1,k=2)$.

假设对于 n，已有相应的 d 及 $id=m_i^{k_i}$，其中 $i=1, 2, \cdots, n$；m_i，$k_i\in\mathbf{N}$，$k_i\geqslant2$.

设 k_1，k_2，$\cdots$，k_n 的最小公倍数是 k，令 $d'=d[(n+1)d]^k$，则有

$id'=id[(n+1)d]^k=m_i^{k_i}[(n+1)d]^k=\{m_i[(n+1)d]^{\frac{k}{k_i}}\}^{k_i},i=1,2,\cdots,n.$

$(n+1)d'=(n+1)d[(n+1)d]^k=[(n+1)d]^{k+1}$.

从而引理对 $n+1$ 成立.

即对所有自然数 n，引理成立. 于是本题得证.

2. 结合其他定理运用中国剩余定理处理问题

例 9 (IMO-46 预选题) 设 a，b 是正整数，使得对于任意的正整数 n，均有 $(a^n+n)\mid(b^n+n)$. 证明：$a=b$.

证明 假设 $b\neq a$.

当 $n=1$ 时，有 $(a+1)\mid(b+1)$，故 $b>a$.

设 p 是一个大于 b 的素数，n 是满足 $n\equiv1(\bmod\ (p-1))$，$n\equiv-a(\bmod\ p)$ 的正整数.

由中国剩余定理知，这样的 n 是存在的. 例如，$n=(a+1)(p-1)+1$.

由费马小定理，有

$a^n=a^{k(p-1)+1}\equiv a(\bmod\ p)$，其中，$k$ 为整数.

所以，$a^n+n\equiv0(\bmod\ p)$.

因此，$p\mid(b^n+n)$.

再由费马小定理，有 $b^n+n\equiv(b-a)(\bmod\ p)$.

所以，$p\mid(b-a)$，矛盾.

因此，$a=b$.

例 10 (2002 年澳大利亚数学奥林匹克题) 设整数 n 和 q 满足 $n\geqslant5$，$2\leqslant q\leqslant n$. 证明：$q-1$ 整除 $\left[\frac{(n-1)!}{q}\right]$，其中 $[x]$ 表示不超过 x 的最大整数.

证明 当 $q<n$ 时，则 $q(q-1)\mid(n-1)!$，所以，

$(q-1)\left|\frac{(n-1)!}{q}=\left[\frac{(n-1)!}{q}\right]\right.$.

当 $q=n$ 时，分两种情况讨论.

(1) 若 q 是素数，由威尔逊 (Wilson) 定理，有

$(n-1)!\equiv-1\equiv n-1(\bmod\ n)$.

因为 $(n-1)!\equiv0\equiv n-1(\bmod\ n-1)$，且 $(n,n-1)=1$，由中国剩余定理，有

$(n-1)!\equiv n-1(\bmod\ n(n-1))$.

于是存在整数 k,使得

$(n-1)!=kn(n-1)+n-1$.

故$\left[\frac{(n-1)!}{q}\right]-\left[k(n-1)+\frac{n-1}{n}\right]=k(n-1)$可以被 $q-1=n-1$ 整除.

(2) 若 q 是合数，设 p 是 n 的最大素因数，且 $n=px$，则 $1<x<n$. 因为 $x \mid n$，且$(n,n-1)=1$,所以，$x\leqslant n-2$.

同理，$p\leqslant n-2$.

若 p 和 x 不同，则 p 和 x 均在$(n-2)!=1\times2\times\cdots\times(n-2)$中的 $n-2$ 项因数中出现,所以，

$n=px\mid(n-2)!$,即 $n(n-1)\mid(n-1)!$.

结论成立.

若 $p=x$，则 $n=p^2$.

因为 $n>4$，则 $p>2$，于是有 $p^2>2p$.

又因为$(2p,n)=p$,$(n-1,n)=1$,所以,$2p\neq n-1$. 于是,$2p\leqslant n-2$,且 p 和 $2p$ 均在$(n-2)!=1\times2\times\cdots\times(n-2)$中的 $n-2$ 项因数中出现. 从而 $2p^2\mid(n-2)!$,即有 $n(n-1)\mid(n-1)!$. 结论成立.

例 11 (2006 年泰国数学奥林匹克题) p_k 表示第 k 个素数，求 $\sum\limits_{k=2}^{2550}p_k^{p_k^4-1}$除以 2550 后所得的余数.

解 用 $\varphi(n)$表示小于或等于 n 的与 n 互素的自然数的个数[如 $\varphi(5)=4$,小于或等于 5 的自然数中 1,2,3,4 与 5 互素].

由于 $2550=2\times3\times5^2\times17$，首先考虑 $p_k\neq2$，3，5，17 时，$p_k^{p_k^4-1}$模 2550 的情况.

因为 $\varphi(5)=4$,$(5,p_k)=1$,所以,由费马小定理知 $5\mid(p_k^4-1)$.

又 $p_k^4-1=(p_k-1)(p_k+1)(p_k^2+1)$,且或者 $4\mid(p_k-1)$,或者 $4\mid(p_k+1)$,则当 $k>1$ 时,$16\mid(p_k^4-1)$.

因此,$20\mid(p_k^4-1)$.

又因为 $\varphi(2)=1$,$\varphi(3)=2$,$\varphi(5^2)=5\times4$,$\varphi(17)=16$,所以,由欧拉定理知

$p_k^{p_k^4-1}\equiv1\pmod 2$,$p_k^{p_k^4-1}\equiv1\pmod 3$,

$p_k^{p_k^4-1}\equiv1\pmod{5^2}$,$p_k^{p_k^4-1}\equiv1\pmod{17}$.

因此,$p_k^{p_k^4-1}\equiv1\pmod{2550}$.

其次考虑 $p_k=2,3,5,17$ 的情况.

因为 $2=p_1$,而所求为 $\sum\limits_{k=2}^{2550}p_k^{p_k^4-1}$,所以,无须考虑 $p_k=2$ 的情况.

又知 $3=p_2$，$5=p_3$，$17=p_7$．为简明起见，记 $A=p_2^{p_2^4-1}$，$B=p_3^{p_3^4-1}$，$C=p_7^{p_7^4-1}$．经简单的计算便知，

$$\begin{cases}A\equiv1,\ 0,\ 1,\ 1\ (\text{mod }2,\ 3,\ 5^2,\ 17),\\ B\equiv1,\ 1,\ 0,\ 1\ (\text{mod }2,\ 3,\ 5^2,\ 17),\\ C\equiv1,\ 1,\ 1,\ 0\ (\text{mod }2,\ 3,\ 5^2,\ 17).\end{cases}$$

[注：$A\equiv1,0,1,1(\text{mod }2,3,5^2,17)$表示 A 对 $2,3,5^2,17$ 分别取模余 1,0,1,1.]

因此，$A+B+C\equiv2(\text{mod }3,5^2,17)$．

故 $A+B+C\equiv2(\text{mod }3\times5^2\times17)$．

又因为 $A+B+C\equiv3\equiv1(\text{mod }2)$，所以，由中国剩余定理知

$A+B+C\equiv2+3\times5^2\times17(\text{mod }2\times3\times5^2\times17)$．

综上，$\sum_{k=2}^{2550}p_k^{p_k^4-1}\equiv(2+3\times5^2\times17)+(2550-4)\equiv1273(\text{mod }2550)$．

例 12 （2006 年意大利国家队选拔考试题）对于每个正整数 n，A_n 表示由正整数组成的集合，其元素 a 满足 $a\leqslant n$，$n\mid(a^n+1)$．

（1）求所有正整数 n，使得 A_n 非空；

（2）求所有正整数 n，使得 $|A_n|$ 是非零的，且为偶数；

（3）是否存在正整数 n，使得 $|A_n|=130$？

解 （1）若 $4\mid n$，则 $a^n+1\equiv1$ 或 $2(\text{mod }4)$，从而，$n\nmid(a^n+1)$．

若 $2\nmid n$，则当 $a=n-1$ 时，

$(n-1)^n+1\equiv(-1)^n+1\equiv0(\text{mod }n)$．

若 $2\parallel n$ 且存在素数 $p\mid n$，$p\equiv3(\text{mod }4)$，则对任意的 a，都有 $p\nmid(a^2+1)$．从而，$n\nmid(a^n+1)$．

若对任意的奇素数 $p\mid n$ 且 $p\equiv1(\text{mod }4)$，下面证明：对任意的素数 $p\equiv1(\text{mod }4)$，存在整数 a，使得

$p^\alpha\mid(a^{2p^{\alpha-1}}+1)$．

显然，存在 a，使得 $p\mid(a^2+1)$．

对 α 归纳．

当 $\alpha=1$ 时，结论显然成立．

假设当 $\alpha=k$ 时，结论成立．

当 $\alpha=k+1$ 时，

$$\frac{a^{2p^k}+1}{a^{2p^{k-1}}+1}=\frac{1-(-a^2)^{p^k}}{1-(-a^2)^{p^{k-1}}}=1+(-a^2)^{p^{k-1}}+(-a^2)^{2p^{k-1}}+\cdots+(-a^2)^{(p-1)p^{k-1}}.$$

又 $(-a^2)^{p^{k-1}}\equiv1(\text{mod }p)$，所以，

$p\left|\dfrac{2^{2p^k}+1}{a^{2p^{k-1}}+1}\right.$.

又 $p^k \mid (a^{2p^{k-1}}+1)$，则 $p^{k+1} \mid (a^{2p^k}+1)$.

设 $n=\prod\limits_{i=1}^{k} p_i^{\alpha_i}$，则存在 a，使得

$p_i \mid (a^2+1)(i=1,2,\cdots,k)$.

从而，$\dfrac{n}{2} \mid (a^n+1)$.

故 $n \mid (a^n+1)$ 或 $n \left| \left[\left(a\pm\dfrac{n}{2}\right)^n+1\right]\right.$.

综上，当 $n=2\prod\limits_{i=1}^{k} p_i^{\alpha_i}$ 且 $p_i\equiv1 \pmod 4$，$\alpha_i\geqslant1$ 或 n 为奇数时，满足条件.

(2) 若 n 为奇数，设 $b=n-a$，则

$n \mid (a^n+1) \Leftrightarrow n \mid (b^n-1)$.

设 $n=\prod\limits_{i=1}^{k} p_i^{\alpha_i}$，$(n,p_i-1)=d_i$.

由费马小定理得 $p_i \mid (b^{p_i-1}-1)$，所以，

$n \mid (b^n-1) \Rightarrow p_i \mid (b^n-1) \Rightarrow p_i \mid (b^{d_i}-1)$.

又 $p_i \mid (b^{d_i}-1) \Rightarrow b^{d_i}=kp_i+1(k\in\mathbf{Z})$

$$\Rightarrow b^{d_i p_i^{\alpha_i-1}}-1=(kp_i+1)^{p_i^{\alpha_i-1}}-1=\sum_{j=1}^{p_i^{\alpha_i-1}} \mathrm{C}_{p_i^{\alpha_i-1}}^{j}(kp_i)^j.$$

显然，当 $j\geqslant2$ 时，$\mathrm{C}_{p_i^{\alpha_i-1}}^{j}$ 中 p_i 的次数 $\geqslant\alpha_i-2$；当 $j=1$ 时，$\mathrm{C}_{p_i^{\alpha_i-1}}^{1}=p_i^{\alpha_i-1}$.

从而，$p_i \mid (b^{d_i}-1) \Rightarrow p_i^{\alpha_i} \mid (b^{d_i p_i^{\alpha_i-1}}-1) \Rightarrow p_i^{\alpha_i} \mid (b^n-1)$.

因此，$p_i^{\alpha_i} \mid (b^n-1) \Leftrightarrow p_i \mid (b^{d_i}-1)$，其中，后者在 $(\bmod\ p_i)$ 中有 d_i 个解.

所以，$b^n\equiv1(\bmod\ p_i^{\alpha_i})$ 在 $(\bmod\ p_i^{\alpha_i})$ 中有 $d_i p_i^{\alpha_i-1}$ 个解 $(i=1,2,\cdots,k)$.

由中国剩余定理的推广，可知 $b^n\equiv1(\bmod\ n)$ 在 $(\bmod\ n)$ 中有 $\prod\limits_{i=1}^{k} d_i p_i^{\alpha_i-1}$ 个解，其为奇数.

若 $2\parallel n$，$n \mid (a^n+1)$，则 $n \mid [(n-a)^n+1]$.

若 $n>2$，则 $|A_n|$ 为偶数.

若 $n=2$，则 $|A_n|$ 为奇数.

(3) 设 $n=2\prod\limits_{i=1}^{k} p_i^{\alpha_i}$，$n=2t$，则

$p_i^{\alpha_i} \mid [(-a^2)^t-1]$，

从而，$p_i \mid [(-a^2)^{\prod_{j\neq i} p_j^{\alpha_j}}-1]$.

显然，上式中的 a (mod p_i) 的解有偶数个.

又 $2 \parallel 130$，有 $k=1$，从而，$n=2p^{\alpha}$.

若 $\alpha \geqslant 3$ 则 $p^2 \mid 130$,矛盾. 所以，$\alpha \leqslant 2$.

若 $\alpha=2$，则 $p \mid 130$,从而，$p=5$ 或 13.

当 $p=5$ 时，$n=2\times 5^2=50<130$，矛盾.

当 $p=13$ 时，$n=2\times 13^2=338$，有

$13^2 \mid (a^{338}+1) \Rightarrow 13 \mid (a^2+1)$,

则共有 $2\times 13=26$ 个解满足要求，矛盾.

若 $\alpha=1$，$2p \mid (a^{2p}+1)$,从而，

$p \mid (a^{2p}+1) \Rightarrow p \mid (a^2+1)$,

则共有 2 个解满足要求，矛盾.

所以，不存在 $n \in \mathbf{Z}_+$，使得 $|A_n|=130$.

【模拟实战】

1. (1978 年罗马尼亚数学奥林匹克题) 设 m 和 n 是自然数，满足：对任意自然数 n，$11k-1$ 与 m 和 $11k-1$ 与 n 具有相同的最大公约数. 证明存在某个整数 l，使得 $m=11^l n$.
2. (1990 年列宁格勒数学奥林匹克题) 设 $F(x)$ 为整系数多项式，今知对任何整数 n，$F(n)$ 都可以被整数 $a_1, a_2, \cdots, a_m$ 之一整除. 证明可以从这些整数中选出一个数来，使得对任何 n，$F(n)$ 都可以被它整除.
3. (1975 年美国纽约数学奥林匹克题) 设整数 a，b，c，d 的最大公约数为 1，试问：$ad-bc$ 的任何素约数都是 a 与 c 的约数的必要且充分条件为，对每个整数 n，$an+b$ 与 $cn+d$ 都互素，对否?
4. (1990 年国家集训队测试题) 能否找到含有 1990 个自然数的集合 S，使
   (1) S 中任意两数互素；
   (2) S 中任意 k ($\geqslant 2$) 个数的和为合数.
5. (2008 年美国数学奥林匹克题) 证明对任意正整数 n，总存在两两互素的大于 1 的整数 k_0，k_1，$\cdots$，k_n，使得 $k_0 k_1 \cdots k_n-1$ 可表示为两个连续整数的乘积.
6. (1955 年第 15 届美国普特南数学竞赛题) 是否存在 1000000 个连续整数，使得每一个都含有二重的素因子，即都能被某个素数的平方所整除.
7. (1982 年第 11 届美国数学奥林匹克题) 证明存在一个正整数 k，使得 $k\cdot 2^n+1$ 对每一个正整数 n，均为合数.

8. (IMO－30 试题) 证明：对任意正整数 r，存在 r 个连续正整数，它们都不是素数的幂.

9. 设 $F(x)$为整系数多项式，已知对任何整数 n，$F(n)$都能被整数 a_1，a_2，…，a_m 之一整除. 证明：可以从这些整数中选出一个数来，使得对任何 n，$F(n)$都可以被它整除.

第十四章　二次剩余

【基础知识】

二次剩余的出现源自解二次同余方程

$$ax^2+bx+c\equiv 0 \pmod p, \qquad ①$$

其中 p 为奇素数，$p\nmid a$.

若要对①进行求解，则将它两边同乘以 $4a$，同加上 b^2，配方得：

$$(2ax+b)^2\equiv b^2-4ac.$$

令 $y=2ax+b$,则 $y^2\equiv b^2-4ac \pmod p$. 显然这个同余方程与①同时有解或无解. 于是，就只须讨论形如 $x^2\equiv d \pmod p$ 的同余方程，注意到当 $p\mid d$ 时，上式只有 $x\equiv 0 \pmod p$ 这一解，所以，以后恒假定 $p\nmid d$，这样便引进了二次剩余.

定义 1　设素数 $p>2$，d 是整数，$p\nmid d$，如果同余方程 $x^2\equiv d \pmod p$ 有解，则称 d 是模 p 的"二次剩余"（亦称平方剩余）；若无解，则称 d 是模 p 的"非二次剩余".

例如，取 $p=5$，那么 $d\equiv 1, -1 \pmod 5$ 是模 5 的二次剩余；取 $p=11$，那么 $d\equiv 1, 3, 4, 5, 9 \pmod{11}$ 是模 11 的二次剩余. 一般地有以下结论：

定理 1　在模 p 的一个简化剩余系中，恰有 $\frac{p-1}{2}$ 个模 p 的二次剩余，$\frac{p-1}{2}$ 个模 p 的非二次剩余. 此外，若 d 是模 p 的二次剩余，则同余方程 $x^2\equiv d \pmod p$ 的解数为 2.

事实上，只要取模 p 的绝对最小简化剩余系

$$-\frac{p-1}{2},\ -\frac{p-1}{2}+1,\ \cdots,\ -1,\ 1,\ \cdots,\ \frac{p-1}{2}-1,\ \frac{p-1}{2} \qquad ②$$

来讨论，d 是模 p 的二次剩余当且仅当

$$d\equiv\left(-\frac{p-1}{2}\right)^2,\left(-\frac{p-1}{2}+1\right)^2,\cdots,(-1)^2,1^2,\cdots,\left(\frac{p-1}{2}-1\right)^2 \text{或} \left(\frac{p-1}{2}\right)^2 \pmod p.$$

由于 $(-j)^2\equiv j^2 \pmod p$,所以 d 是模 p 的二次剩余当且仅当

$$d\equiv 1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}-1\right)^2,\ \left(\frac{p-1}{2}\right)^2 \pmod p. \qquad ③$$

上式给出了模 p 的全部二次剩余，共有$\frac{p-1}{2}$个，由于模 p 的简化剩余系有 $p-1$ 个数，所以另外的$\frac{p-1}{2}$个数必为模 p 的非二次剩余.

当 d 是模 p 的二次剩余时，注意到 $1\leqslant i<j\leqslant\frac{p-1}{2}$时，$i^2\not\equiv j^2\pmod p$，结合③知，必有唯一的 i，$1\leqslant i\leqslant\frac{p-1}{2}$，使 $x\equiv i(\mathrm{mod}\ p)$是 $x^2\equiv d(\mathrm{mod}\ p)$的解，进而推出在简化剩余系②中有且仅有 $x\equiv\pm i(\mathrm{mod}\ p)$是 $x^2\equiv d(\mathrm{mod}\ p)$的解，即同余方程 $x^2\equiv d(\mathrm{mod}\ p)$的解数为 2，定理得证.

需要指明 x^2 恰能取$\{0,1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2\}$共$\frac{p-1}{2}+1$个值，即模 p 的完系中有$\frac{p+1}{2}$个二次剩余.

我们关心的是，对于什么样的 d，它是 mod p 的二次剩余.

定理 2　(欧拉判别法)

设素数 $p>2$，$p\nmid d$，那么，d 是模 p 的二次剩余的充要条件是

$$d^{\frac{p-1}{2}}\equiv1(\mathrm{mod}\ p);\qquad ④$$

d 是模 p 的非二次剩余的充要条件是

$$d^{\frac{p-1}{2}}\equiv-1(\mathrm{mod}\ p).\qquad ⑤$$

事实上，首先可证明对任一 d，$p\nmid d$，式④或⑤有且仅有一式成立，由费马小定理知 $d^{p-1}\equiv1(\mathrm{mod}\ p)$，因而有$(d^{\frac{p-1}{2}}-1)(d^{\frac{p-1}{2}}+1)\equiv0(\mathrm{mod}\ p)$. 由于素数 $p>2$ 及$(d^{\frac{p-1}{2}}-1,\ d^{\frac{p-1}{2}}+1)\mid2$，所以推出④或⑤式有且仅有一式成立.

下面讨论 d 是模 p 的二次剩余的充要条件是④成立，先看必要性.

若 d 是模 p 的二次剩余，则必有 x_0 使得

$d\equiv x_0^2(\mathrm{mod}\ p)$，因而有 $x_0^{p-1}\equiv d^{\frac{p-1}{2}}(\mathrm{mod}\ p)$.

由于 $p\nmid d$，所以 $p\nmid x_0$，由费马小定理知

$d^{\frac{p-1}{2}}\equiv x_0^{p-1}\equiv1(\mathrm{mod}\ p)$，必要性得证.

再看充分性，设④式成立，这时必有 $p\nmid d$. 考虑一次同余方程 $ax\equiv b(\mathrm{mod}\ p)$，由 $p\nmid d$ 知对于由②式给出的模 p 的简化剩余系中的每个 j，当 $a=j$ 时，必有唯一的 $x=x_j$属于简化剩余系②使得 $ax\equiv b(\mathrm{mod}\ p)$成立. 若 d 不是模 p 的二次剩余，必有 $j\neq x_j$，这样，简化剩余系②中的 $p-1$ 个数即可按 j，x_j 一对，两两分完，因此有

$d^{\frac{p-1}{2}}\equiv(p-1)!\equiv-1(\mathrm{mod}\ p)$（利用了 Wilson 定理).

但这与④矛盾，所以必有某一 j_0，使 $j_0=x_{j_0}$，从而 d 是模 p 的二次剩余，充分

性得证.

这样便完成了对欧拉判别式的推证.

定义 2 设素数 $p>2$，定义整变数 d 的函数

$$\left(\frac{d}{p}\right)=\begin{cases}1, 当 d 是模 p 的二次剩余; \\ -1, 当 d 是模 p 的非二次剩余; \\ 0, 当 p \mid d.\end{cases}$$

则把 $\left(\frac{d}{p}\right)$ 称为 Legendre 符号. 由上述定理 2，则可以立即推出，Legendre 符号具有以下性质：

(i) $\left(\frac{d}{p}\right)=\left(\frac{p+d}{p}\right)$；

(ii) $\left(\frac{d}{p}\right)\equiv d^{\frac{p-1}{2}}(\bmod p)$；

(iii) $\left(\frac{1}{p}\right)=1, \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$；

(iv) $\left(\frac{dc}{p}\right)=\left(\frac{d}{p}\right)\cdot\left(\frac{c}{p}\right)$.

【典型例题与基本方法】

例 1 （第 5 届香港数学奥林匹克题）设 p 是满足 $p\equiv 1(\bmod 4)$ 的奇素数，计算 $\sum_{k=1}^{p-1}\left\{\frac{k^2}{p}\right\}$ 的值，其中 $\{x\}=x-[x]$，$[x]$ 为不超过 x 的最大整数.

解 注意到 $(-k)^2\equiv(p-k)^2\equiv k^2(\bmod p)$.

若 $x^2\equiv y^2(\bmod p)$，其中 $1\leqslant x, y\leqslant\frac{p-1}{2}$，则

$(x-y)(x+y)\equiv 0(\bmod p)$.

由于 $1<x+y<p$，所以，$x=y$.

这表明 $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ 是模 p 的二次剩余.

因为 $p\equiv 1(\bmod 4)$，由欧拉准则 $\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\equiv 1(\bmod p)$ 知，-1 是模 p 的二次剩余.

由 $\left(\frac{-b}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{b}{p}\right)$，得 b 是模 p 的二次剩余的充分必要条件为 $-b\equiv p-b(\bmod p)$ 也是模 p 的二次剩余. 所以，集合 $\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}$ 在模 p 意义下为集

合$\{a_1, p-a_1, a_2, p-a_2, \cdots, a_{\frac{p-1}{4}}, p-a_{\frac{p-1}{4}}\}$.

当$1\leqslant a_i, p-a_i<p$时，有

$$\left\{\frac{a_i}{p}\right\}+\left\{\frac{p-a_i}{p}\right\}=\frac{a_i+p-a_i}{p}=1.$$

于是，所求和式为$\frac{p-1}{4}$.

例 2 （第 16 届韩国数学奥林匹克题）设 m 是正整数.

(1) 如果 $2^{m+1}+1$ 整除 $3^{2^m}+1$，证明：$2^{m+1}+1$ 是素数；

(2) (1) 的逆命题是否成立？

证明 (1) 设 $q=2^{m+1}+1$.

根据题中的条件，可得

$$3^{2^m}\equiv-1 \pmod q. \qquad ①$$

由此可知，$(3,q)=1$.

将式①两边平方，得

$$3^{2^{m+1}}\equiv1 \pmod q.$$

设 k 是满足 $3^k\equiv1 \pmod q$的最小正整数，那么，k 是 $2^{m+1}=q-1$ 的因子.

于是，k 具有 2^r 的形式，其中 r 是某个满足 $r\leqslant m+1$ 的正整数. 假定 $r\leqslant m$，则 $3^{2^m}\equiv1 \pmod q$，这与式①矛盾.

因此，必有 $r=m+1$.

另一方面，由欧拉定理，k 是 $\varphi(q)$的因子，于是，$2^{m+1}=q-1$ 整除 $\varphi(q)$.

由于 $\varphi(q)\leqslant q-1$，可得 $\varphi(q)=q-1$.

因而，q 是素数.

(2) 设 $q=2^{m+1}+1$ 是素数，则

$$\varphi(q)=q-1=2^{m+1}.$$

由于 $q\geqslant5$，可得$(3,q)=1$. 由费尔马小定理，有 $3^{\varphi(q)}=3^{2^{m+1}}\equiv1 \pmod q$. 于是，

$$3^{\frac{\varphi(q)}{2}}=3^{2^m}\equiv\pm1 \pmod q. \qquad ②$$

由于 $q\equiv1 \pmod 4$，以及 $q\equiv2 \pmod 3$，有

$$\left(\frac{3}{q}\right)=(-1)^{\frac{(3-1)(q-1)}{4}}\left(\frac{q}{3}\right)=\left(\frac{2}{3}\right)=-1,$$其中$\left(\frac{*}{*}\right)$是 Legendre 符号.

另外，由于$-1=\left(\frac{3}{q}\right)\equiv3^{\frac{(q-1)}{2}} \pmod q$，故式②的值应取$-1$.

因此，$q\mid(3^{2^m}+1)$.

这就证明了 (1) 的逆命题.

【解题思维策略分析】

1. 适时运用二次剩余

例 3 （第 38 届奥地利数学奥林匹克题）求所有非负整数 a （$a<2007$），使得 $x^2+a\equiv0 \pmod{2007}$ 恰有两个不同且小于 2007 的非负整数解.

解 因为 $2007=3^2\times223$，所以，

$x^2+a\equiv0 \pmod{2007}$.

在模 2007 意义下的解的数目等于 $x^2+a\equiv0 \pmod 9$ 和 $x^2+a\equiv0 \pmod{223}$ 解的数目的乘积.

因为 $x^2\equiv0,1,4,7 \pmod 9$，所以

当 $a\in\{1,3,4,6,7\}$ 时，$x^2+a\equiv0 \pmod 9$，无解；

当 $a\in\{2,5,8\}$ 时，有两个解；

当 $a=0$ 时，有三个解.

如果 $-a\in S=\{b_i \mid b_i\equiv i^2 \pmod{223}, 0<b_i<223, i=1,2,\cdots,111\}$，则

$x^2+a\equiv0 \pmod{223}$ 有两个解；

如果 $-a\notin S\cup\{0\}$，则无解；

当 $a=0$ 时，有一个解.

因此，原同余方程有两个解时只可能是 $x^2+a\equiv0 \pmod 9$ 有两个解，$x^2+a\equiv0 \pmod{223}$ 有一个解.

设 $a=223b$.

因为 $223\equiv-2 \pmod 9$，-2 是模 9 的二次剩余，所以，$-b$ 也是模 9 的二次剩余.

于是，$b=2$，5，8.

故 $a=2\times223=446$，$a=5\times223=1115$，$a=8\times223=1784$.

例 4 （2004 年新加坡数学奥林匹克题）求有序整数对 (a,b) 的个数，使得 $x^2+ax+b=167y$ 有整数解 (x,y)，其中 $1\leqslant a,b\leqslant2004$.

解 先证明一个引理.

引理 p 为奇素数，当 x 取遍模 p 的完全剩余系时，x^2 模 p 恰能取到 0，1，$\cdots$，$p-1$ 中的 $\frac{p+1}{2}$ 个值.

引理的证明：$x\equiv0 \pmod p$ 时，$x^2\equiv0 \pmod p$.

当 $p\nmid x$ 时，

若 $x_1^2\equiv x_2^2 \pmod p$，$x_1\not\equiv x_2 \pmod p$，则有

$p\mid(x_1+x_2)(x_1-x_2)$，$p\mid(x_1+x_2)$.

所以，$x_1\equiv\quad x_2 \pmod p$.

这样，将 1，2，…，$p-1$ 分成$\frac{p-1}{2}$组

$(1,p-1),(2,p-2),\cdots,\left(\frac{p-1}{2},\frac{p+1}{2}\right)$.

同组数的平方模 p 相等，不同组数的平方模 p 不相等.

因此，二次剩余恰能取到 $1+\frac{p-1}{2}-\frac{p+1}{2}$个值.

接下来求解原题.

当存在 $x\in\mathbf{Z}$，使 $x^2+ax+b\equiv0 \pmod{167}$时，则有整数解$(x,y)$，即

$4x^2+4ax+4b\equiv0 \pmod{167}$，

$a^2-4b\equiv(2x+a)^2 \pmod{167}$.

因此，a 取一个值时，a^2-4b 取模 167 的二次剩余.

由引理 a^2-4b 模 167 能取到 84 个不同的值，所以，b 模 167 能取 84 个不同的值.

又因为$\frac{2004}{167}=12$，故每个 a 对应 84×12 个满足要求的 b，因此，共有

$2004\times84\times12=2020032$

个有序整数对.

数列 a_0，a_1，a_2，…定义如下：

对于所有的 $k(k\geqslant0)$，

$a_0=2$，$a_{k+1}=2a_k^2-1$.

2. 善于运用 Legendre 符号

例 5 （*2002 年第 10 届土耳其数学奥林匹克题*）找出所有的素数 p，使得满足 $0\leqslant x$，$y\leqslant p$，且 $y^2\equiv x^3-x \pmod p$的整数对(x,y)恰有 p 对.

解 我们引入 Legendre 符号$\left(\frac{a}{p}\right)$：

p 为奇素数，$(a,p)=1$；

$$\left(\frac{a}{p}\right)=\begin{cases}1,\text{当 } x^2\equiv a \pmod p \text{ 有解时},\\-1,\text{当 } x^2\equiv a \pmod p \text{ 无解时}.\end{cases}$$

注意到 Legendre 符号的如下性质：

(1) $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$，

(2) $\left(\frac{-1}{p}\right)=\begin{cases}1,p\equiv1 \pmod 4,\\-1,p\equiv\quad 1 \pmod 4.\end{cases}$

又注意到定理 1，即注意到如下结论：

若$(a,p)=1$，p为奇素数，$x^2\equiv a(\bmod p)$有解，则它有且仅有两解.

事实上，设$x\equiv x_0$是一解，则$x\equiv -x_0$也是一解. 又p是奇数，则$x_0\not\equiv -x_0(\bmod p)$. 所以，至少有两解.

若另有一解x_1，且$x_1\not\equiv x_0$，$x_1\not\equiv -x_0(\bmod p)$，则

$x_0^2\equiv x_1^2(\bmod p)$，

$(x_0-x_1)(x_0+x_1)\equiv 0(\bmod p)$.

所以，$p\mid(x_0-x_1)$或$p\mid(x_0+x_1)$. 矛盾.

因此，仅有两解.

下面证明原题.

记$f(x)=x^3-x$，则$f(x)$是奇函数.

当$p=2$时，$y^2\equiv f(x)(\bmod p)$恰有两解$(0,0)$，$(1,0)$.

当$p\equiv 3(\bmod 4)$时，因为$\left(\frac{-a}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)=-\left(\frac{a}{p}\right)$，所以，

$y^2\equiv f(x)$与$y^2\equiv -f(x)\equiv f(-x)$一个有解，一个无解.

设$x=2，3，\cdots，\frac{p-1}{2}$中，$y^2\equiv f(x)$有$k$个有解，则$x=\frac{p+1}{2},\frac{p+3}{2},\cdots,p-2$中，$y^2\equiv f(x)$有$\frac{p-3}{2}-k$个有解.

所以，$x=2,3,\cdots,p-2$中，$y^2\equiv f(x)$有$\frac{p-3}{2}$个有解.

又由引理它们有两个解，则$x=2,3,\cdots,p-2$中，有$p-3$组解.

当$x=0,1,p-1$时，$y^2\equiv f(x)\equiv 0(\bmod p)$各有一组解.

所以，共有p组解.

当$p\equiv 1(\bmod 4)$时，

因为$\left(\frac{-a}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)=\left(\frac{a}{p}\right)$，所以，$y^2\equiv f(x)$与$y^2\equiv f(-x)$或同有两个解或同无解.

设$x=2,3,\cdots,\frac{p-1}{2}$中，$y^2\equiv f(x)$有$k$个有解，则$x=\frac{p+1}{2},\frac{p+3}{2},\cdots,p-2$中，$y^2\equiv f(x)$有$k$个有解.

所以，$x=2,3,\cdots,p-2$中，$y^2\equiv f(x)(\bmod p)$有$4k$组解.

当$x=0,1,p-1$时，$y^2\equiv f(x)\equiv 0(\bmod p)$各有一组解.

所以，共有$4k+3$组解.

但$p\neq 4k+3$，所以，$p\equiv 1(\bmod 4)$必不满足条件.

综上所述，$p=2$ 或 $p\equiv3\pmod 4$.

例 6 （2003 年新加坡数学奥林匹克题）对于给定的素数 p，判断方程

$$x^2+y^2+pz=2003$$

是否总有整数解 x，y，z？并证明你的结论.

解 为证原题先给出如下引理.

引理 每个与 1 模 4 同余的素数均可写为两个平方数的和.

事实上，首先，引入 Legendre 记号 $\left(\frac{a}{p}\right)$，其中 p 为奇素数，且 $(a,p)=1$，则

(i) 当 $x^2\equiv a \pmod p$ 有解时，$\left(\frac{a}{p}\right)=1$；

(ii) 当 $x^2\equiv a \pmod p$ 无解时，$\left(\frac{a}{p}\right)=-1$.

注意到 Legendre 记号的如下性质：

(1) $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$.

(2) $\left(\frac{-1}{p}\right)=\begin{cases}1, p\equiv1 \pmod 4;\\ -1, p\equiv-1 \pmod 4.\end{cases}$

因为 $p\equiv1 \pmod 4$，故 $\left(\frac{-1}{p}\right)=1$.

所以，存在 $u\in\mathbf{Z}$，使得

$$u^2+1\equiv0 \pmod p.$$

故存在某个 $k(k\geqslant1)$，满足 $u^2+1=kp$，即存在 $k(k\geqslant1)$，使

$$kp=x^2+y^2\ (x,y\in\mathbf{Z}).$$

令 $r\equiv x \pmod k$，$s\equiv y \pmod k$，$-\frac{k}{2}<r,s\leqslant\frac{k}{2}$，则 $r^2+s^2\equiv x^2+y^2\equiv0 \pmod k$，即存在 $k_1\in\mathbf{N}$，使得

$$r^2+s^2=k_1k.$$

从而，$(r^2+s^2)(x^2+y^2)=k_1k\cdot kp=k_1k^2p$.

又 $(r^2+s^2)(x^2+y^2)=(rx+sy)^2+(ry-sx)^2$，故

$$\left(\frac{rx+sy}{k}\right)^2+\left(\frac{ry-sx}{k}\right)^2=k_1p.$$

由于 $rx+sy\equiv x^2+y^2\equiv0 \pmod k$，

$ry-sx\equiv xy-yx\equiv0 \pmod k$，

所以，$\frac{rx+sy}{k}$ 与 $\frac{ry-sx}{k}$ 都是整数，从而，k_1p 也可表示为两个数的平方和的

形式.

因为 $k_1k=r^2+s^2\leqslant\left(\frac{k}{2}\right)^2+\left(\frac{k}{2}\right)^2=\frac{k^2}{2}$，则 $k_1\leqslant\frac{k}{2}<k$.

故只要 $k\neq1$，总存在一个 $k_1<k$，使得 k_1p 也可表示为两个数的平方和的形式.因此，p 可表示为两个数的平方和.

下面证明原题.

若 $p\neq2003$ 且 $p\neq2$，则

$(2003,2p)=1,(2003+2p,4p)=1.$

由狄利克莱定理知，数列$\{2003+2p+4pn\}$包含无限多个素数.

取其中任一个 $q=2003+4pn_0+2p$.

由于 $2003+4pn_0+2p\equiv1(\mathrm{mod}\ 4)$，故

$q\equiv1(\mathrm{mod}\ 4)$.

由引理可知，q 可表示为 x^2+y^2 的形式$(x,y\in\mathbf{Z})$，故

$x^2+y^2+p(-4n_0-2)=2003.$

取 $z=-4n_0-2$，即有

$x^2+y^2+pz=2003.$

若 $p=2003$，取 $x=y=0$，$z=1$；

若 $p=2$，取 $x=1$，$y=0$，$z=1001$.

所以，方程 $x^2+y^2+pz=2003$ 总有解.

注　下面给出狄利克莱定理.

狄利克莱定理　若$(a,b)=1$，则$\{an+b\}$包含有无限多个素数.

【模拟实战】

1. 设 k 是一个正整数. 证明：存在无穷多个形如 $n\cdot2^k-7$ 的完全平方数，其中 n 为正整数.
2. 不存在整数 x，y 使得 $x^2+3xy-2y^2=122$.
3. 不存在一对正整数 x，y 满足 $3y^2=x^4+x$.
4. (1) 证明：当素数 $p=4m+3$，$\left(\frac{a}{p}\right)=1$ 时，$x_0=\pm a^{m+1}$ 是 $x^2\equiv a(\mathrm{mod}\ p)$的解；

   (2) 当 $p=8m+5$，$\left(\frac{a}{p}\right)=1$ 时，求 $x^2\equiv a(\mathrm{mod}\ p)$的解.
5. 证明：有无穷多个 $4k+1$ 型的素数.
6. 证明：有无穷多个 $8k+1$ 型的素数.
7. (2004 年国家队培训题) 求所有具有如下性质的函数 $f:\{1,2,\cdots,n,\cdots\}\to\mathbf{Z}$：

(1) 若 a，b 是正整数，且 $a|b$，则 $f(a)\geqslant f(b)$；

(2) 若 a，b 是正整数，则 $f(ab)+f(a^2+b^2)=f(a)+f(b)$.

8. (2008 年国家队培训题) 求出正整数 n 可以表示为两个互素的整数的平方和的充要条件.

9. 设 p 是奇素数. 证明：-1 是模 p 的平方剩余的充要条件是 $p\equiv 1 \pmod 4$.

10. 设 $p>3$ 是素数，A_l 表示集合 $\{1,2,\cdots,p-1\}$ 中两两不同的 l 个正整数的乘积之和，即

$A_1=1+2+\cdots+(p-1)$，

$A_2=1\cdot 2+1\cdot 3+\cdots+(p-2)(p-1)$，

……

$A_{p-1}=(p-1)!$.

证明：

(1) 当 $1\leqslant l\leqslant p-2$ 时，$A_l\equiv 0 \pmod p$；

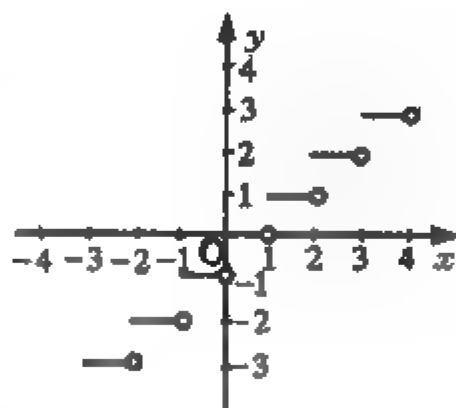
(2) 当 $1<l<p$ 且 l 为奇数时，$A_l\equiv 0 \pmod {p^2}$.

11. (2000 年国家集训队测试题) 已知 p 为大于 3 的奇数，$a>b>1$. 求证：$C_{ap}^{bp}\equiv C_a^b \pmod {p^3}$.

第十五章 高斯函数 $[x]$

【基础知识】

1. 定义：设 $x\in\mathbf{R}$，则 $[x]$ 为不大于 x 的最大整数．其图象如右所示．



2. 函数 $[x]$ 的性质：

(1) $y=[x]$ 的定义域为实数集 $\mathbf{R}$，值域为整数集 $\mathbf{Z}$.

(2) $x=[x]+r$，$0\leqslant r<1$.

(3) $x-1<[x]\leqslant x<[x]+1$.

(4) $y=[x]$ 是广义增函数，即当 $x_1\leqslant x_2$ 时，$[x_1]\leqslant[x_2]$ 成立；

(5) 设 $n\in\mathbf{Z}$，则 $[n+x]=n+[x]$（即整数可以外移或内移）.

(6) $\left[\sum\limits_{i=1}^{n}x_i\right]\geqslant\sum\limits_{i=1}^{n}[x_i]$. 特别地 $[nx]\geqslant n[x]$，其中 n 为正整数.

(7) 对正实数 x_1，x_2，…，x_n 有 $\left[\prod\limits_{i=1}^{n}x_i\right]\geqslant\prod\limits_{i=1}^{n}[x_i]$. 特别地，对正数 x 及正整数 n 有 $[x^n]\geqslant[x]^n$，$[x]\geqslant[\sqrt[n]{x}]^n$.

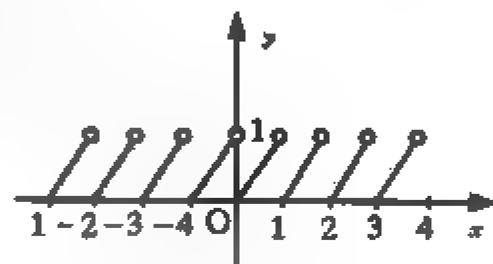
(8) 对正实数 x，y 有 $\left[\dfrac{y}{x}\right]\leqslant\dfrac{[y]}{[x]}$.

(9) 设 n 为正整数，则 $\left[\dfrac{x}{n}\right]=\left[\dfrac{[x]}{n}\right]$.

(10) 对整数 x，$[-x]=-[x]$，对非整数 x，$[-x]=-[x]-1$.

(11) 对正整数 m 和 n，不大于 m 的 n 的倍数共有 $\left[\dfrac{m}{n}\right]$ 个.

(12) 函数 $\{x\}$：$\{x\}$ 定义为实数 x 的正的纯小数部分，即 $\{x\}=x-[x]$. 其图象如右所示.



$y=\{x\}$ 还有如下一些性质：

$\{x\}\in[0,1)$；

$\{x\}$ 是以 1 为最小正周期的周期函数；

$\{n+x\}=\{x\}$,(n 为整数).

【典型例题与基本方法】

例 1 (第 9 届美国数学邀请赛 AIME 试题)设 r 是实数且满足条件:

$\left[r+\frac{19}{100}\right]+\left[r+\frac{20}{100}\right]+\left[r+\frac{21}{100}\right]+\cdots+\left[r+\frac{91}{100}\right]=546.$

求$[100r]$.

解 设$[r]=n$,且设$\left[r+\frac{19}{100}\right],\left[r+\frac{20}{100}\right],\cdots,\left[r+\frac{91}{100}\right]$中有 k 个为 $n+1$,$73-k$ 个 n,($0\leqslant k\leqslant 73$).

于是按题意,有$(73-k)n+k(n+1)=546$,即 $n=7+\frac{35-k}{73}$,所以 $k=35$,$n=7$.

这样便得 $r+\frac{56}{100}<8$, $r+\frac{57}{100}\geqslant 8$, 即 $743\leqslant 100r<744$.

故 $[100r]=743$.

例 2 (第 17 届全俄中学生数学竞赛第 3 阶段试题)证明:对任意的自然数 n,数 $1+[(3+\sqrt{5})^n]$被 2^n 整除.

证明 设 $x_n=(3+\sqrt{5})^n+(3-\sqrt{5})^n$,$n\geqslant 1$, 则

$x_{n+2}=[(3+\sqrt{5})+(3-\sqrt{5})]\cdot[(3+\sqrt{5})^{n+1}+(3-\sqrt{5})^{n+1}]-[(3+\sqrt{5})\cdot(3-\sqrt{5})^{n+1}+(3-\sqrt{5})(3+\sqrt{5})^{n+1}]=6x_{n+1}-4x_n$,

即 $x_{n+2}=6x_{n+1}-4x_n(n\geqslant 1)$. (*)

因 $x_1=6$, $x_2=28$, 都是整数, 由(*)知所有 x_n 都是整数.

又因 $0<3-\sqrt{5}<1$, 则

$x_n=(3+\sqrt{5})^n+(3-\sqrt{5})^n=1+[(3+\sqrt{5})^n]$.

现用数学归纳法证明 x_n 被 2^n 整除.

当 $n=1$ 和 $n=2$ 时, 命题成立.

假设 $n=k$ 和 $n=k+1$ 时命题成立, 即 $x_k=2^kp$, $x_{k+1}=2^{k+1}p$, 其中, p, $q\in\mathbf{N}$.

由(*)$x_{k+2}=2^{k+2}(3p-q)$,即 x_{k+2}被 2^{k+2}整除, 因此命题得证.

例 3 (2003 年克罗地亚国家数学竞赛题)对于所有素数 p 和所有正整数 n($n\geqslant p$). 证明: $C_n^p-\left[\frac{n}{p}\right]$能被 p 整除.

证明 用 N 表示 n, $n-1$, $\cdots$, $n-p+1$ 中唯一可能被 p 整除的整数, 那么,$\left[\frac{n}{p}\right]=\frac{N}{p}$. 于是,

$$C_n^p-\left[\frac{n}{p}\right]=\frac{n(n-1)\cdots(N+1)N(n-1)\cdots(n-p+1)}{p!}-\frac{N}{p}$$

$$=\frac{N}{p!}[n(n-1)\cdots(N+1)(N-1)\cdots(n-p+1)-(p-1)!]. \qquad ①$$

数 n，$n-1$，…，$N+1$，$N-1$，…，$n-p+1$ 模 p 不余零，且余数各不相同. 因此，它们的积为

$$n(n-1)\cdots(N+1)(N-1)\cdots(n-p+1)\equiv(p-1)!\ (\mathrm{mod}\ p).$$

这就意味着式①中括号里的表达式能被 p 整除. 因此，数

$$A=\frac{n(n-1)\cdots(N+1)N(N-1)\cdots(n-p+1)}{p}-\frac{N(p-1)!}{p}$$

也能被 p 整除（因为它是式①中括号内表达式的$\frac{N}{p}$倍）.

作为一个素数，p 和$(p-1)!$ 互素. 因此，数

$$C_n^p-\left[\frac{n}{p}\right]=\frac{1}{(p-1)!}\cdot A$$

能被 p 整除.

例 4 求证：在 $n!$ 的素因数分解式中，素数 p 的指数是 $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots+\left[\frac{n}{p^m}\right]$$(p^m\leqslant n\leqslant p^{m+1})$.

证明 由于 p 是素数，因此 $n!$ 中含 p 的指数 $p(n!)$一定是 1，2，…，$n-1$，n 各数中所含 p 的指数的总和. 易知，1，2，…，n 中有$\left[\frac{n}{p}\right]$个 p 的倍数，有$\left[\frac{n}{p^2}\right]$个 p^2 的倍数，…，所以

$$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots.$$

此例说明：$n!=p^{p(n!)}\cdot M$,其中 M 不含 p 的因数. 例如，由于

$$7(2000!)=\left[\frac{2000}{7}\right]+\left[\frac{2000}{7^2}\right]+\cdots=285+40+5=330,$$

则 $2000!=7^{330}\cdot M$，其中 $7\nmid M$.

例 5（1981 年美国数学竞赛题）对自然数 n 和一切实数 x，求证：

$$[nx]\geqslant\frac{[x]}{1}+\frac{[2x]}{2}+\cdots+\frac{[nx]}{n}.$$

证明 用数学归纳法，为叙述方便，设

$$A_n=\frac{[x]}{1}+\frac{[2x]}{2}+\cdots+\frac{[nx]}{n}.$$

(1) 当 $n=1$ 时，$[nx]=[x]$，$A_n=\frac{[x]}{1}=[x]$. 原不等式成立.

(2) 假设当 $k<n$ 时，原不等式成立，即已证
$A_1\leqslant[x],A_2\leqslant[2x],\cdots,A_{n-1}\leqslant[(n-1)x]$.

由于 $A_k-A_{k-1}=\frac{[kx]}{k}$，则 $kA_k-kA_{k-1}=[kx]$.

令 $k=1,2,\cdots,n$，得
$nA_n-nA_{n-1}=[nx]$,
$(n-1)A_{n-1}-(n-1)A_{n-2}=[(n-1)x]$,
……
$2A_2-2A_1=[2x],A_1=[x]$.
两边分别相加，得
$nA_n-(A_1+A_2+\cdots+A_{n-1})=[x]+[2x]+\cdots+[nx]$,
即 $nA_n=[x]+[2x]+\cdots+[(n-1)x]+[nx]+A_{n-1}+A_{n-2}+\cdots+A_2+A_1$.
由归纳假设知
$nA_n\leqslant[x]+[2x]+\cdots+[(n-1)x]+[nx]$.

例 6 (CMO-6 试题) 求所有自然数 n，使得

$\min\limits_{k\in \mathbf{N}}\left(k^2+\left[\frac{n}{k^2}\right]\right)=1991(n\in \mathbf{N})$.

解 题给条件等价于：对一切 $k\in \mathbf{N}$,
$k^2+(n/k^2)\geqslant1991$, ①
且存在 $k\in \mathbf{N}$，使得 $k^2+(n/k^2)<1992$. ②
而①等价于对一切 $k\in \mathbf{N}$,

$k^4-1991k^2+n\geqslant0$，即 $(k^2-1991/2)^2+n-\frac{1991^2}{4}\geqslant0$.

因 $[\sqrt{1991/2}]=31$，而 $31^2-\frac{1991}{2}=-\frac{69}{2}$，$32^2-\frac{1991}{2}=\frac{57}{2}$,

故上式左边在 $k=32$ 时最小，因此①等价于
$n\geqslant1991\cdot32^2-32^4=1024\cdot967$.
又②等价于存在 $k\in \mathbf{N}$，使 $(k^2-996)^2+n-996^2<0$.
上式左边亦在 $k=32$ 时最小，故②等价于
$n<1992\cdot32^2-32^4=1024\cdot968$.
故所求的一切 n 为：$1024\cdot967\leqslant n\leqslant1024\cdot967+1023$ ($n\in \mathbf{N}$).

例 7 (2005 年巴尔干数学奥林匹克题) 设 m，n 是互素的正整数，且 m 为偶

数，n 为奇数．证明：和 $\frac{1}{2n}+\sum_{k=1}^{n-1}(-1)^{\left[\frac{mk}{n}\right]}\left\{\frac{mk}{n}\right\}$ 不依赖于 m，n，其中 $[x]$ 为不超过 x 的最大整数，$\{x\}=x-[x]$，空项的和为 0.

证明　我们证明

$$S=\sum_{k=1}^{n-1}(-1)^{\left[\frac{mk}{n}\right]}\left\{\frac{mk}{n}\right\}=\frac{1}{2}-\frac{1}{2n}.$$

这表明，所给的和等于 $\frac{1}{2}$.

为方便计算 S，对任何 $k\in\{1,2,\cdots,n-1\}$，记 $mk=n\left[\frac{mk}{n}\right]+r_k$，其中 $r_k\in\{1,2,\cdots,n-1\}$.

可以导出：

(1) 由于 m，n 互素，故 r_k 是互不相同的．于是，

$\{r_1,r_2,\cdots,r_{n-1}\}=\{1,2,\cdots,n-1\}$.

(2) $\left\{\frac{mk}{n}\right\}=\frac{r_k}{n}(k=1,2,\cdots,n-1)$.

(3) 由于 m 是偶数，n 是奇数，则 $\left[\frac{mk}{n}\right]\equiv r_k(\bmod 2)$.

于是，$(-1)^{\left[\frac{mk}{n}\right]}=(-1)^{r_k}(k=1,2,\cdots,n-1)$.

因此，$S=\frac{1}{n}\sum_{k=1}^{n-1}(-1)^{r_k}r_k=\frac{1}{n}\sum_{k=1}^{n-1}(-1)^k k=\frac{1}{2}-\frac{1}{2n}$.

【解题思维策略分析】

1. 运用函数[x]的性质证明含[f(n)]的恒等式、不等式

例 8　（1987 年第 19 届加拿大数学竞赛题）对每一正整数 n，证明

$[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+1}]=[\sqrt{4n+2}]=[\sqrt{4n+3}]$.

证明　设 x 为正整数，且 $x^2>4n+1$.

若 x 为偶数，则 $x^2=4m>4n+1$，因而

$m\geqslant n+1$,

$x^2=4m\geqslant 4n+4>4n+3$.

同样有 $x^2>4n+2$.

若 x 为奇数，则

$x^2=4m+1>4n+1$.

同样有 $x^2>4n+3$.

特别地，取 $x=[\sqrt{4n+1}]+1$，则有

$[\sqrt{4n+1}]+1>\sqrt{4n+3}>\sqrt{4n+1}\geqslant[\sqrt{4n+1}]$,

所以 $[\sqrt{4n+3}]=[\sqrt{4n+1}]$,

从而 $[\sqrt{4n+1}]=[\sqrt{4n+2}]=[\sqrt{4n+3}]$.

另一方面,

$(\sqrt{n}+\sqrt{n+1})^2=2n+1+2\sqrt{n(n+1)}>2n+1+2n=4n+1$,

$(\sqrt{n}+\sqrt{n+1})^2<2n+1+2(n+1)=4n+3$.

所以有 $4n+1<(\sqrt{n}+\sqrt{n+1})^2<4n+3$，即

$[\sqrt{4n+1}]\leqslant[\sqrt{n}+\sqrt{n+1}]\leqslant[\sqrt{4n+3}]$.

于是有

$[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+1}]=[\sqrt{4n+2}]=[\sqrt{4n+3}]$.

例 9 （1994 年第 12 届美国数学邀请赛题）对实数 x，$[x]$表示不超过 x 的最大整数. 求使$[\log_2 1]+[\log_2 2]+[\log_2 3]+\cdots+[\log_2 n]=1994$ 成立的正整数 n.

解 令 $S_n=\sum\limits_{i=1}^{n}[\log_2 i]$.

注意到，对非负整数 k，有 2^k 个正整数 x，使$[\log_2 x]=k$,即 $x=2^k$，2^k+1，…，$2^{k+1}-1$.

所以，对正整数 r，有

$$S_{2^r-1}=0+(1+1)+(2+2+2+2)+\cdots+[\underbrace{(r-1)+(r-1)+\cdots+(r-1)}_{2^{r-1}\text{个}}]$$

$$=1\cdot 2+2\cdot 2^2+\cdots+(r-1)\cdot 2^{r-1}$$

$$=(r-1)\cdot 2^r-(2^r-2)$$

$$=(r-2)\cdot 2^r+2.$$

令 $r=8$，得 $S_{255}=1538<1994$,

令 $r=9$，得 $S_{511}=3586>1994$.

因此，如果 $S_n=1994$，那么 $2^8-1<n<2^9-1$,

$1994=S_n=S_{255}+(n-255)\cdot 8=1538+8n-255\times 8=8n-502$.

所以 $n=312$.

例 10 （1981 年第 44 届莫斯科数学奥林匹克题）试问：对 $x>1$，下面的等式

$[\sqrt{[\sqrt{x}]}]=[\sqrt{\sqrt{x}}]$

一定能成立吗?

解 由函数$[a]$的定义得

$[\sqrt{\sqrt{x}}]\leqslant\sqrt{\sqrt{x}}<[\sqrt{\sqrt{x}}]+1$.

设$[\sqrt{\sqrt{x}}]=n$，则有$n^4\leqslant x<(n+1)^4$，从而

$$n^2\leqslant\sqrt{x}<(n+1)^2,$$

$$n^2\leqslant[\sqrt{x}]<(n+1)^2,$$

$$n\leqslant\sqrt{[\sqrt{x}]}<n+1,$$

$$n\leqslant[\sqrt{[\sqrt{x}]}]<n+1,$$

因此　$[\sqrt{[\sqrt{x}]}]=n$. 于是　$[\sqrt{[\sqrt{x}]}]=[\sqrt{\sqrt{x}}]$.

例 11　(CMO-23 试题) 给定正整数 n，及实数 $x_1\leqslant x_2\leqslant\cdots\leqslant x_n$，$y_1\geqslant y_2\geqslant\cdots\geqslant y_n$，满足 $\sum\limits_{i=1}^{n}ix_i=\sum\limits_{i=1}^{n}iy_i$.

证明：对任意实数 α，有 $\sum\limits_{i=1}^{n}x_i[i\alpha]\geqslant\sum\limits_{i=1}^{n}y_i[i\alpha]$，这里，$[\beta]$表示不超过实数 β 的最大整数.

证法 1　我们先证明一个引理.

引理　对任意实数 α 和正整数 n，有 $\sum\limits_{i=1}^{n-1}[i\alpha]\leqslant\frac{n-1}{2}[n\alpha]$.

引理的证明：只需要将$[i\alpha]+[(n-i)\alpha]\leqslant[n\alpha]$对 $i=1, 2, \cdots, n-1$ 求和即得.

回到原题，我们采用归纳法对 n 进行归纳.

当 $n=1$ 时显然正确.

假设 $n=k$ 时原命题成立，考虑 $n=k+1$. 令 $a_i=x_i+\frac{2}{k}x_{k+1}$，$b_i=y_i+\frac{2}{k}y_{k+1}$，其中 $i=1, 2, \cdots, k$. 显然我们有 $a_1\leqslant a_2\leqslant\cdots\leqslant a_k$，$b_1\geqslant b_2\geqslant\cdots\geqslant b_k$，并且通过计算得知 $\sum\limits_{i=1}^{k}ia_i=\sum\limits_{i=1}^{k}ib_i$，由归纳假设知$\sum\limits_{i=1}^{k}a_i[i\alpha]\geqslant\sum\limits_{i=1}^{k}b_i[i\alpha]$.

又 $x_{k+1}\geqslant y_{k+1}$，否则若 $x_{k+1}<y_{k+1}$，则

$$x_1\leqslant x_2\leqslant\cdots\leqslant x_{k+1}<y_{k+1}\leqslant\cdots\leqslant y_2\leqslant y_1,$$

由已知有 $\sum\limits_{i=1}^{k+1}ix_i=\sum\limits_{i=1}^{k+1}iy_i$，矛盾！从而

$$\begin{aligned}\sum_{i=1}^{k+1}x_i[i\alpha]-\sum_{i=1}^{k}a_i[i\alpha]&=x_{k+1}\left\{[(k+1)\alpha]-\frac{2}{k}\sum_{i=1}^{k}[i\alpha]\right\}\\&\geqslant y_{k+1}\left\{[(k+1)\alpha]-\frac{2}{k}\sum_{i=1}^{k}[i\alpha]\right\}\\&=\sum_{i=1}^{k+1}y_i[i\alpha]-\sum_{i=1}^{k}b_i[i\alpha],\end{aligned}$$

由此可得 $\sum_{i=1}^{k+1} x_i[i\alpha] \geqslant \sum_{i=1}^{k+1} y_i[i\alpha]$. 由归纳法知原命题对任意正整数 n 均成立.

证法 2 记 $z_i = x_i - y_i$，则 $z_1 \leqslant z_2 \leqslant \cdots \leqslant z_n$ 且 $\sum_{i=1}^{n} iz_i = 0$，只需要证明

$$\sum_{i=1}^{n} z_i[i\alpha] \geqslant 0. \qquad ①$$

令 $\Delta_1 = z_1$，$\Delta_2 = z_2 - z_1$，…，$\Delta_n = z_n - z_{n-1}$，则 $z_i = \sum_{j=1}^{i} \Delta_j (1 \leqslant i \leqslant n)$，所以

$$0 = \sum_{i=1}^{n} iz_i = \sum_{i=1}^{n} i \sum_{j=1}^{i} \Delta_j = \sum_{j=1}^{n} \Delta_j \sum_{i=j}^{n} i,$$

从而

$$\Delta_1 = -\frac{\sum_{j=2}^{n} \Delta_j \sum_{i=j}^{n} i}{\sum_{i=1}^{n} i}, \qquad ②$$

于是

$$\begin{aligned}\sum_{i=1}^{n} z_i[i\alpha] &= \sum_{i=1}^{n} [i\alpha] \sum_{j=1}^{i} \Delta_j = \sum_{j=1}^{n} \Delta_j \sum_{i=j}^{n} [i\alpha] \\ &= \sum_{j=2}^{n} \Delta_j \sum_{i=j}^{n} [i\alpha] - \sum_{j=2}^{n} \Delta_j \cdot \frac{\sum_{i=j}^{n} i}{\sum_{i=1}^{n} i} \cdot \sum_{i=1}^{n} [i\alpha] \\ &= \sum_{j=2}^{n} \Delta_j \sum_{i=j}^{n} i \cdot \left(\frac{\sum_{i=j}^{n} [i\alpha]}{\sum_{i=j}^{n} i} - \frac{\sum_{i=1}^{n} [i\alpha]}{\sum_{i=1}^{n} i} \right).\end{aligned}$$

故①转化为只要证明对任意的 $2 \leqslant j \leqslant n$，

$$\frac{\sum_{i=j}^{n} [i\alpha]}{\sum_{i=j}^{n} i} \geqslant \frac{\sum_{i=1}^{n} [i\alpha]}{\sum_{i=1}^{n} i}. \qquad ③$$

而

$$③ \Leftrightarrow \frac{\sum_{i=j}^{n} [i\alpha]}{\sum_{i=j}^{n} i} \geqslant \frac{\sum_{i=1}^{j-1} [i\alpha]}{\sum_{i=1}^{j-1} i} \Leftrightarrow \frac{\sum_{i=1}^{n} [i\alpha]}{\sum_{i=1}^{n} i} \geqslant \frac{\sum_{i=1}^{j-1} [i\alpha]}{\sum_{i=1}^{j-1} i},$$

故只需要证明对任意的 $k \geqslant 1$，有

$$\frac{\sum_{i=1}^{k+1}[i\alpha]}{\sum_{i=1}^{k+1}i}\geqslant\frac{\sum_{i=1}^{k}[i\alpha]}{\sum_{i=1}^{k}i}.$$

而上述不等式等价于

$$[(k+1)\alpha]\cdot\frac{k}{2}\geqslant\sum_{i=1}^{k}[i\alpha]\Leftrightarrow\sum_{i=1}^{k}([(k+1)\alpha]-[i\alpha]-[(k+1-i)\alpha])\geqslant 0,$$

注意到$[x+y]\geqslant[x]+[y]$对任意实数x，y成立，上述不等式显然成立．从而③得证．

例 12 （2005 年国家集训队选拔考试题）设n是任意给定的正整数，x是正实数．证明：

$\sum_{k=1}^{n}\left(x\left[\frac{k}{x}\right]-(x+1)\left[\frac{k}{x+1}\right]\right)\leqslant n$，其中$[a]$表示不超过实数$a$的最大整数．

证明 首先证明一个引理．

引理 对任意实数α及$\beta>0$，有整数u及实数v使得

$\alpha=\beta u+v$，其中$0\leqslant v<\beta$，

并且上述u及v唯一确定．

引理的证明：取$u=\left[\frac{\alpha}{\beta}\right]$及$v=\alpha-\beta\left[\frac{\alpha}{\beta}\right]$，则易知$0\leqslant v<\beta$．此外，若另有整数$u'$及实数$v'(0\leqslant v'<\beta)$，满足$\alpha=\beta u'+v'$，则

$\beta(u-u')=v'-v.$

因上式左边的绝对值或是 0 或不小于β；而右边的绝对值小于β，故必须$u=u'$，及$v'=v$．

这就证明了所说的唯一性．

现在回到原题．由引理知，对任意的$k=1, 2, \cdots, n$，有

$$k=a_kx+b_k=c_k(x+1)+d_k,\qquad ①$$

这里$a_k=\left[\frac{k}{x}\right]$，$c_k=\left[\frac{k}{x+1}\right]$，$0\leqslant b_k<x$，$0\leqslant d_k<x+1$．

记不等式左边的和为S，则

$$\begin{aligned}S&=\sum_{k=1}^{n}(a_kx-c_k(x+1))\\&=\sum_{k=1}^{n}((k-b_k)-(k-d_k))\\&=\sum_{k=1}^{n}d_k-\sum_{k=1}^{n}b_k.\qquad ②\end{aligned}$$

记 $I=\{1\leqslant k\leqslant n|d_k>1\}$，令 $f(k)=k-c_k-1$. 因当 $k\in I$ 时，有

$k=c_k(x+1)+d_k>c_k+1$,

故 $0<f(k)<n$，即 f 是 I 到集合 $\{1,2,\cdots,n\}$ 的一个映射. 我们证明 f 必是单射. 事实上，若有 $k,l\in I(k\neq l)$ 使 $f(k)=f(l)$，则 $k-l=c_k-c_l$，结合①易知

$$(c_k-c_l)x=d_l-d_k. \qquad ③$$

另一方面，因 k，$l\in I$，故 d_k，$d_l\in(1,x+1)$，从而 $|d_k-d_l|<|x|$. 但 $|c_k-c_l|\cdot|x|=|k-l|\cdot|x|\geqslant|x|$，从而③式两边绝对值不等. 矛盾！

此外，由 $k=c_k(x+1)+d_k$ 易知 $f(k)=c_kx+(d_k-1)$.

因当 $k\in I$ 时，有 $0<d_k-1<x$，故由引理中的唯一性知 $c_k=a_{f(k)}$ 及 $d_k-1=b_{f(k)}$.

因此，由②可知（注意对所有 k 有 $b_k\geqslant 0$）

$$S=\sum_{k\in I}d_k+\sum_{k\notin I}d_k-\sum_{k=1}^{n}b_k\leqslant\sum_{k\in I}d_k-\sum_{k\in I}d_{f(k)}+\sum_{k\notin I}d_k$$

$$=\sum_{k\in I}(d_k-b_{f(k)})+\sum_{k\notin I}d_k=\sum_{k\in I}1+\sum_{k\notin I}d_k\leqslant|I|+(n-|I|)=n.$$

2. 运用函数$[x]$的性质解含$[a]$的方程、不等式

例 13 （1998 年加拿大数学奥林匹克题）求满足方程 $\left[\frac{a}{2}\right]+\left[\frac{a}{3}\right]+\left[\frac{a}{5}\right]=a$ 的实数 a.

解 由 $x-1<[x]\leqslant x$，可得

$$a>\left(\frac{a}{2}-1\right)+\left(\frac{a}{3}-1\right)+\left(\frac{a}{5}-1\right)=\frac{31}{30}a-3,$$

$$a\leqslant\frac{a}{2}+\frac{a}{3}+\frac{a}{5}=\frac{31}{30}a,$$

即 $\frac{31}{30}a-3<a\leqslant\frac{31}{30}a$,

所以 $0\leqslant a<90$.

又 a 是非负整数，故有

$$a\geqslant\left(\frac{a}{2}-\frac{1}{2}\right)+\left(\frac{a}{3}-\frac{2}{3}\right)+\left(\frac{a}{5}-\frac{4}{5}\right)=\frac{31}{30}a-\frac{59}{30},$$

因而 $a\leqslant 59$.

由题设可知 $\frac{a}{2}-\left\{\frac{a}{2}\right\}+\frac{a}{3}-\left\{\frac{a}{3}\right\}+\frac{a}{5}-\left\{\frac{a}{5}\right\}=a$，即

$$\left\{\frac{a}{2}\right\}+\left\{\frac{a}{3}\right\}+\left\{\frac{a}{5}\right\}=\frac{1}{30}a. \qquad (※)$$

由于 $\left\{\frac{a}{2}\right\}=0,\frac{1}{2}$,

又$\left\{\frac{a}{3}\right\}=0,\frac{1}{3},\frac{2}{3}$,且$\left\{\frac{a}{5}\right\}=0,\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5}$.

(※) 式共有 $2\times3\times5=30$ 个结果.

又 $15i+10j+6k(i=0,1;j=0,1,2,;k=0,1,2,3,4)$是方程的解,

所以 $a=15i+10j+6k(i=0,1;j\ \ 0,1,2;k=0,1,2,3,4)$.

例 14 (IMO 37 预选题) 求满足下式的所有自然数 a 和 b:

$$\left[\frac{a^2}{b}\right]+\left[\frac{b^2}{a}\right]=\left[\frac{a^2+b^2}{ab}\right]+ab.$$

解 由对称性,不妨设 $a\leqslant b$.

由 $x-1<[x]\leqslant x$,有

$$\frac{b^2}{a}+\frac{a^2}{b}-2<\left[\frac{a^2}{b}\right]+\left[\frac{b^2}{a}\right]\leqslant\frac{a^2}{b}+\frac{b^2}{a},$$

及 $$ab+\frac{a^2+b^2}{ab}-1<\left[\frac{a^2+b^2}{ab}\right]+ab\leqslant\frac{a^2+b^2}{ab}+ab,$$

即 $$-1<\frac{a^2}{b}+\frac{b^2}{a}-\frac{a^2+b^2}{ab}-ab<2,$$ 或

$$-ab<a^3+b^3-a^2-b^2-a^2b^2<2ab,$$

整理得 $$\begin{cases}b^3-(a^2+1)b^2-2ab+a^3-a^2<0, & ①\\ b^3-(a^2+1)b^2+ab+a^3-a^2>0. & ②\end{cases}$$

先考虑①式,

若 $b\geqslant a^2+2$,则

$$\begin{aligned}&b^3-(a^2+1)b^2-2ab+a^3-a^2\\=&b[b(b-a^2-1)-2a]+a^3-a^2\geqslant b(b-2a)+a^3-a^2\\=&(b-a)^2+a^3-2a^2\geqslant(a^2-a+2)^2+a^3-2a^2\\=&(a^2-a+2)^2-a^2+a^2(a-1)\\=&(a^2+2)(a^2-2a+2)+a^2(a-1)>0,\end{aligned}$$

与①式矛盾. $b\geqslant a^2+2$ 不真,于是 $b\leqslant a^2+1$.

再考虑②式,

设 $f(x)=x^3-(a^2+1)x^2+ax+a^3-a^2$.

当 $a\geqslant2$ 时,有 $f(-a)=-a^3-(a^2+1)a^2-a^2+a^3-a^2<0$.

又 $f(0)=a^3-a^2>0$,且 $f(a)=a^2(-a^2+2a-1)<0$,

而 $f(a^2)=a^2(-a^2+2a-1)<0$,

同时 $f(a^2+1)=a(2a^2-a+1)>0$.

因此,方程 $f(x)=0$ 的三个根在区间$(-a,0)$,$(0,a)$,(a^2,a^2+1)中各有一个.

故,当 $a\leqslant b\leqslant a^2$ 时,有 $f(b)<0$,与②式矛盾. 于是 $b\geqslant a^2+1$.

当 $a=1$ 时，②式化为 $b^3-2b^2+b>0$，

即 $b(b-1)^2>0$，所以 $b\geqslant 2=a^2+1$.

总之，若②式成立，则 $b\geqslant a^2+1$.

综上，只能有 $b=a^2+1$.

将 $b=a^2+1$ 代入原式得

$$\left[\frac{a^2}{a^2+1}\right]+\left[\frac{a^4+2a^2+1}{a}\right]=\left[\frac{a^2+1}{a}+\frac{1}{a^2+1}\right]+a(a^2+1).$$

当 $a\geqslant 2$ 时，上式化为 $a^3+2a=a+a(a^2+1)$，这是一个恒等式.

当 $a=1$ 时，上式化为

$$\left[\frac{1}{2}\right]+\left[\frac{1+2+1}{1}\right]=\left[\frac{2}{1}+\frac{1}{2}\right]+(1+1),$$

此时显然成立.

因此，$a\leqslant b$ 时，原方程的所有解为 $b=a^2+1$，$a\in\mathbf{N}$.

同理，$b\leqslant a$ 时，原方程的所有解为 $a=b^2+1$，$b\in\mathbf{N}$.

因此，原方程的所有解为

$b=a^2+1$，$a\in\mathbf{N}$，或 $a=b^2+1$，$b\in\mathbf{N}$.

例 15 （IMO-39 预选题）确定所有的实数对 (a,b) 使得 $a[bn]=b[an]$ 对一切正整数 n 成立.

解 令 $n=1$，得 $a[b]=b[a]$， ①

设 $a=[a]+\{a\}$，$b=[b]+\{b\}$，其中 $\{a\}$，$\{b\}$ 为 a，b 的小数部分，则由已知有

$a[[b]n+\{b\}n]=b[[a]n+\{a\}n]$，

$a[b]n+a[\{b\}n]=b[a]n+b[\{a\}n]$.

由①得 $a[\{b\}n]=b[\{a\}n]$. ②

存在自然数 k，使 $\{a\}<\frac{1}{k}$，令 $n=k$，由②得

$a[k\{b\}]=0$. ③

若 $a\neq 0$，则由③可得 $\{b\}<\frac{1}{k}$.

这就表明，当 a 为整数(即 $\{a\}=0$)时，b 必为整数.

同样，若 $b\neq 0$，且 $\{b\}<\frac{1}{k}$，则 $\{a\}<\frac{1}{k}$.

于是，当 a，b 都不是整数时，存在 k，使得

$\frac{1}{k+1}\leqslant\{a\}<\frac{1}{k}$，$\frac{1}{k+1}\leqslant\{b\}<\frac{1}{k}$.

令 $n=k+1$，则

$1\leqslant n\{b\}<\frac{k+1}{k}<2, 1\leqslant n\{a\}<\frac{k+1}{k}<2.$

由②式可得　$a=b$.

由此可得，本题的解为

$(0,a),(a,0),(a,a)$(当 a 为任意实数时)；

(a,b)(当 a,b 均为整数时).

例 16　(1999 年加拿大数学奥林匹克题) 求方程 $4x^2-40[x]+51=0$ 的所有实数解.

解法 1　因为$[x]\leqslant x$,所以

$0=4x^2-40[x]+51\geqslant 4x^2-40x+51=(2x-3)(2x-17)$,

即$\frac{3}{2}\leqslant x\leqslant\frac{17}{2}$.

于是$[x]=1, 2, 3, 4, 5, 6, 7, 8$.

当$[x]=1$时，方程化为 $4x^2+11=0$，无实数解.

当$[x]=2$时，方程化为 $4x^2-29=0$.

由$\frac{3}{2}\leqslant x\leqslant\frac{7}{2}$得 $x=\frac{\sqrt{29}}{2}$.

当$[x]=3$时，可得 $x=\frac{\sqrt{69}}{2}$，与$[x]=3$矛盾；

当$[x]=4$时，可得 $x=\frac{\sqrt{109}}{2}$，与$[x]=4$矛盾；

当$[x]=5$时，可得 $x=\frac{\sqrt{149}}{2}$，与$[x]=5$矛盾；

当$[x]=6$时，可得 $x=\frac{\sqrt{189}}{2}$，此时$\left[\frac{\sqrt{189}}{2}\right]=6$，因此,$x=\frac{\sqrt{189}}{2}$是方程的解；

当$[x]=7$时，可得 $x=\frac{\sqrt{229}}{2}$，此时$\left[\frac{\sqrt{229}}{2}\right]=7$，因此,$x=\frac{\sqrt{229}}{2}$是方程的解；

当$[x]=8$时，可得 $x=\frac{\sqrt{269}}{2}$，此时$\left[\frac{\sqrt{269}}{2}\right]=8$，因此,$x=\frac{\sqrt{269}}{2}$是方程的解.

由以上知，题设方程的解集为$\left\{\frac{\sqrt{29}}{2},\frac{\sqrt{189}}{2},\frac{\sqrt{229}}{2},\frac{\sqrt{269}}{2}\right\}$.

解法 2　由性质 (3) 知$[x]\leqslant x<[x]+1$.

又由$[x]<0$不是方程的解,得

$$\begin{cases}4([x]+1)^2-40[x]+51>0,\\4[x]^2-4[x]+51\leqslant 0,\end{cases}$$

即 $\begin{cases}(2[x]-5)(2[x]-11)>0,\\(2[x]-3)(2[x]-7)\leqslant 0,\end{cases}$

解得 $\begin{cases}[x]<\frac{5}{2},\\[x]\geqslant\frac{3}{2},\\[x]\leqslant\frac{17}{2},\end{cases}$ 或 $\begin{cases}[x]>\frac{11}{2},\\[x]\geqslant\frac{3}{2},\\[x]\leqslant\frac{17}{2}.\end{cases}$

从而$[x]=2$或$[x]=6$或$[x]=7$或$[x]=8$，分别代人方程得 $x=\frac{\sqrt{29}}{2}$，或 $x=\frac{\sqrt{189}}{2}$，或 $x=\frac{\sqrt{229}}{2}$，或 $x=\frac{\sqrt{269}}{2}$. 经检验知，这4个值都是原方程的解.

例17 （2006年伊朗国家队选拔考试题）设 n 是一个确定的自然数.

(1) 求方程 $\sum_{k=1}^{n}\left[\frac{x}{2^k}\right]=x-1$ 的所有解；

(2) 当 m 是一个已知自然数时，求方程 $\sum_{k=1}^{n}\left[\frac{x}{2^k}\right]=x-m$ 的所有解的数目.

解 (1) 令 $x=\sum_{i=0}^{\infty}c_i2^i(c_i\in\{0,1\})$，则

$$\sum_{k=1}^{\infty}\left[\frac{x}{2^k}\right]=\sum_{k=1}^{\infty}\sum_{i=k}^{\infty}c_i2^{i-k}=\sum_{i=1}^{\infty}\sum_{k=1}^{i}c_i2^{i-k}=\sum_{i=1}^{\infty}c_i\sum_{k=1}^{i}2^{i-k}$$
$$=\sum_{i=1}^{\infty}c_i(2^i-1)=\sum_{i=0}^{\infty}c_i2^i-\sum_{i=0}^{\infty}c_i=x-f(x),$$

其中，$f(x)$表示 x 二进制表示中“1”的个数.

又 $\sum_{k=1}^{\infty}\left[\frac{x}{2^k}\right]\geqslant\sum_{k=1}^{n}\left[\frac{x}{2^k}\right]$，从而，$f(x)=1$.

设 $x=2^k$，则$\left[\frac{2^k}{2^{n+1}}\right]=0$.

从而，$k\leqslant n$.

所以，$x=2^k(0\leqslant k\leqslant n)$.

(2) 设 $x=2^ny+\sum_{i=1}^{l}2^{r_i}$，其中，$0\leqslant r_1<r_2<\cdots<r_l\leqslant n-1$，则

$$x-\sum_{k=1}^{n}\left[\frac{x}{2^k}\right]=x-(2^ny-y+\sum_{i=1}^{l}2^{r_i}-l)=y+l=m.$$

对特定的 l，$y=m-l$，其中，$0\leqslant l\leqslant m$.

对特定的 l，r_1，r_2，…，r_l 的取法共 C_n^l 种.

因此，方程所有解的数目为 $\sum_{i=0}^{m} C_n^i$.

例 18 （2005 年国家集训队测试题）求所有正整数 m，n，使得不等式

$$[(m+n)\alpha]+[(m+n)\beta]\geqslant[m\alpha]+[m\beta]+[n(\alpha+\beta)] \qquad ①$$

对任意实数 α，β 都成立. 这里 $[x]$ 表示实数 x 的整数部分.

解 答案为 $m=n$.

若 $m=n$，则原不等式为

$$[2m\alpha]+[2m\beta]\geqslant[m\alpha]+[m\beta]+[m(\alpha+\beta)], \qquad ②$$

令 $x=m\alpha$，$y=m\beta$，则上式为

$$[2x]+[2y]\geqslant[x]+[y]+[x+y],$$

即 $[2\{x\}]+[2\{y\}]\geqslant[\{x\}+\{y\}]$.

不妨设 $x\geqslant y$，则 $[2\{x\}]+[2\{y\}]\geqslant[2\{x\}]\geqslant[\{x\}+\{y\}]$，从而②式成立.

反过来，设不等式①对所有 α，β 成立，取 $\alpha=\beta=\frac{1}{m+n+1}$，得 $\left[\frac{2n}{m+n+1}\right]\leqslant 0$，故 $2n<m+n+1$，即 $n\leqslant m$.

另一方面，设 $d=(m,n)$，由裴蜀等式，可取 x，y 为非负整数，满足 $nx=my+m-d$ [可先取正整数 x'，y'，使 $my'-nx'=d\Rightarrow m(y'-1)-nx'=d-m$]. 在①中取 $\alpha=\beta=\frac{x}{m}$，则

$$2\left[\frac{xn}{m}\right]\geqslant\left[\frac{2xn}{m}\right],$$

从而 $2\left\{\frac{xn}{m}\right\}\leqslant\left\{\frac{2xn}{m}\right\}<1$,

故 $\left\{\frac{xn}{m}\right\}<\frac{1}{2}$,

即 $\left\{\frac{my+m-d}{m}\right\}<\frac{1}{2}$,

即 $\frac{m-d}{m}<\frac{1}{2}$,

于是 $m<2d$.

因 $d\mid m$，从而 $m=d$（设 $m=dq$，则由 $dq<2d$ 知 $q=1$），故 $m\mid n$，所以 $m\leqslant n$.

综上所述，知 $m=n$.

3. 运用函数 $[x]$ 的性质求解含 $[x]$ 的各类杂题

例 19 （2008 年全国高中数学联赛题）设集合 $P=\{1,2,3,4,5\}$. 对任意 $k\in P$ 和正整数 m，记 $f(m,k)=\sum_{i=1}^{5}\left[m\sqrt{\frac{k+1}{i+1}}\right]$，其中 $[a]$ 表示不大于 a 的最大整数.

求证：对任意正整数 n，存在 $k\in P$ 和正整数 m，使得 $f(m,k)=n$.

证明 定义集合 $A=\{m\sqrt{k+1}\mid m\in\mathbf{N}^*,k\in P\}$，其中 $\mathbf{N}^*$ 为正整数集.

由于当任意 k，$i\in P$ 且 $k\neq i$ 时，$\frac{\sqrt{k+1}}{\sqrt{i+1}}$ 是无理数，所以对任意的 k_1，$k_2\in P$ 和正整数 m_1，m_2，$m_1\sqrt{k_1+1}=m_2\sqrt{k_2+1}$，当且仅当 $m_1=m_2$，$k_1=k_2$. 这表明 A 中无重复元素.

注意到 A 是一个无穷集，现将 A 中的元素按从小到大的顺序排成一个无穷数列. 对于任意的正整数 n，设此数列中第 n 项为 $m\sqrt{k+1}$. 下面确定 n 与 m，k 间的关系.

若 $m_i\sqrt{i+1}\leqslant m\sqrt{k+1}$，则 $m_i\leqslant m\frac{\sqrt{k+1}}{\sqrt{i+1}}$.

由 m_i 是正整数知，对 $i=1,2,3,4,5$，满足这个条件的 m_i 的个数为 $\left[m\frac{\sqrt{k+1}}{\sqrt{i+1}}\right]$，从而

$$n=\sum_{i=1}^{5}\left[m\frac{\sqrt{k+1}}{\sqrt{i+1}}\right]=f(m,k).$$

因此对任意 $n\in\mathbf{N}^*$，存在 $m\in\mathbf{N}^*$，$k\in P$，使得 $f(m,k)=n$.

例 20 （1997 年第 26 届美国数学奥林匹克题）设非负整数列 a_1，a_2，…，a_{1997} 满足 $a_i+a_j\leqslant a_{i+j}\leqslant a_i+a_j+1$，对所有 i，$j\geqslant 1$，$i+j\leqslant 1997$.

求证：存在唯一实数 x，使得对一切 $n=1,2,\cdots,1997$，$a_n=[nx]$.

证明 若 $a_n=[nx]$ 存在，则

$nx-1<a_n\leqslant nx<a_n+1$.

因而 $\frac{a_n}{n}\leqslant x<\frac{a_n+1}{n}$，即 $x\in\left[\frac{a_n}{n},\frac{a_n+1}{n}\right)$.

我们取定 $x=\max\frac{a_n}{n}$，则只需证明对于一切 $1\leqslant m\leqslant 1997$，

$\frac{a_n}{n}\leqslant x<\frac{a_m+1}{m}$，即 $\frac{a_n}{n}<\frac{a_m+1}{m}$，

因而 $na_m+n>ma_n$. （※）

我们用数学归纳法证明（※）式.

当 $m=n=1$ 时，（※）式成立.

假设 m，n 均小于 k 时，（※）式成立.

当 m，n 中较大的一个为 k 时，有两种情况：

(1) 当 $n=k$ 时，设 $n=qm+r$，$q\in\mathbf{N}$，$0\leqslant r\leqslant m$.

由已知不等式有

$a_n\leqslant a_{qm}+a_r+1\leqslant a_{(q-1)m}+a_m+a_r+2\leqslant\cdots\leqslant qa_m+a_r+q$.

又由归纳假设 $ra_m+r>ma_r$，于是

$$ma_n\leqslant mqa_m+ma_r+qm<mqa_m+ra_m+r+qm$$
$$=(mq+r)a_m+(mq+r)=na_m+n.$$

所以，(※) 式成立.

(2) 当 $m=k$ 时，设 $m=qn+r$，$q\in\mathbf{N}$，$0\leqslant r<m$.

由已知不等式有

$a_m=a_{qn+r}\geqslant a_{qn}+a_r\geqslant a_{(q-1)n}+a_n+a_r\geqslant\cdots\geqslant qa_n+a_r$，

则　$na_m\geqslant nqa_n+na_r$.

而　$na_m+n\geqslant nqa_n+na_r+n=(m-r)a_n+na_r+n=ma_n+na_r+n-ra_n$，

由归纳假设 $na_r+n>ra_n$，

于是　$na_m+n\geqslant ma_n+na_r+n-ra_n>ma_n$.

所以，(※) 式成立. 从而本题得证.

例 21　(1989 年理科实验班入学数学复试题) 通项为 $a_n=b[\sqrt{n+c}]+d$ 的数列，逐次算得各项是

1，3，3，3，5，5，5，5，5，…

其中每一个正奇数 m 恰好连续出现 m 次. 上述 b，c，d 是待定的整数. 求 $b+c+d$ 的值.

解　由于 $a_{n+1}-a_n=b[\sqrt{n+1+c}]-b[\sqrt{n+c}]$，且 a_n 是奇数，$a_{n+1}\geqslant a_n$，则 $a_{n+1}-a_n\in\{0,2\}$，即 $b[\sqrt{n+1+c}]-b[\sqrt{n+c}]=0$ 或 2.

对任何自然数 n，恒有

$$[\sqrt{n+1+c}]-[\sqrt{n+c}]\in\{0,1\}. \qquad ①$$

显然，$b\neq 0$.

当 $a_{n+1}-a_n=2$ 时，即 $b([\sqrt{n+1+c}]-[\sqrt{n+c}])=2$ 时，由①知，只能有

$[\sqrt{n+1+c}]-[\sqrt{n+c}]=1$.

因此　$b=2$.

由于 b 是常数，所以 $b=2$.

下面求 c.

由 $a_1=b[\sqrt{1+c}]+d=2[\sqrt{1+c}]+d$ 可知，$c\geqslant -1$.

由题设数列的特征，我们有 $a_{k^2}=2k-1$.

取充分大的 k，使 $2k+3>c$，这时

$(k+1)^2+c<(k+1)^2+2k+3=(k+2)^2$，从而有

$$[\sqrt{(k+1)^2+c}]<k+2. \quad ②$$

另一方面，又有 $a_{(k+1)^2}=2(k+1)-1$，则

$a_{(k+1)^2}-a_1=[2(k+1)-1]-1=2k$，即

$2[\sqrt{(k+1)^2+c}]-2[\sqrt{1+c}]=2k$，即

$[\sqrt{(k+1)^2+c}]-[\sqrt{1+c}]=k$.

由不等式②，有$[\sqrt{1+c}]<2$，因此 $c<3$.

从而$-1\leqslant c<3$，$c=-1,0,1,2$.

若 $c=0,1,2$，则均有

$a_5-a_4=[\sqrt{5+c}]-[\sqrt{4+c}]=2-2=0$，与 $a_5-a_4=2$ 矛盾.

于是，只能有 $c=-1$.

下面求 d.

由 $a_1=2[\sqrt{1+c}]+d=1$，可知 $d=1$.

因此，$b+c+d=2+(-1)+1=2$.

例 22 （第 17 届日本数学奥林匹克题）$[r]$ 表示不超过 r 的最大整数. 对任意正实数 x，集合 $A(x)$ 定义为：$A(x)=\{[nx]|n\in\mathbf{N}_+\}$.

求所有大于 1 的无理数 α，使得：若正实数 β 满足 $A(\alpha)\supset A(\beta)$，则 $\frac{\beta}{\alpha}$ 为整数.

证明 首先来看：任意大于 2 的无理数 α 满足题目条件.

设 $A(\alpha)\supset A(\beta)$，$[\beta]=[m\alpha](m\in\mathbf{N}_+)$.

用数学归纳法证明：对任意的正整数 k 有$[k\beta]=[km\alpha]$.

当 $k=1$ 时，命题显然成立.

假设 $k=s$ 时，命题成立.

当 $k=s+1$ 时，设$[(s+1)\beta]=[l\alpha](l\in\mathbf{N}_+)$. 只需证明 $l=(s+1)m$.

由$[m\alpha]+[sm\alpha]\leqslant\beta+s\beta<[m\alpha]+[sm\alpha]+2$ 及$[l\alpha]\leqslant(s+1)\beta<[l\alpha]+1$，得

$[l\alpha]<[m\alpha]+[sm\alpha]+2<[l\alpha]+3$，即$[l\alpha]-1\leqslant[m\alpha]+[sm\alpha]\leqslant[l\alpha]$.

因此，有

$$\begin{aligned}(s+1)m\alpha-2&<[m\alpha]+[sm\alpha]\leqslant[l\alpha]\leqslant l\alpha<[l\alpha]+1\\&\leqslant[m\alpha]+[sm\alpha]+2\leqslant(s+1)m\alpha+2.\end{aligned}$$

故$-2<[l-(s+1)m]\alpha<2$.

又由于 $\alpha>2$，则 $l=(s+1)m$.

因此，对任意的正整数 k 有$[k\beta]=[km\alpha]$.

从而，$\beta=m\alpha$，即$\frac{\beta}{\alpha}$为整数.

其次证明：任意大于1、小于2的无理数α不满足题意.

设$\beta=\frac{\alpha}{2-\alpha}$，则$\frac{\beta}{\alpha}=\frac{1}{2-\alpha}$不是整数.

令$m=[n\beta]\in A(\beta)(n\in\mathbf{N}_+)$，则

$m\leqslant n\beta<m+1\Leftrightarrow 2m-m\alpha\leqslant n\alpha<(2m+2)-(m+1)\alpha$，

即$m\leqslant\frac{m+n}{2}\alpha<\frac{n+m+1}{2}\alpha<m+1$.

因$m+n$与$m+n+1$中必有一个偶数，所以，$m\in A(\alpha)$.

因此，$A(\alpha)\supset A(\beta)$，与题目条件矛盾.

综上，本题答案为大于2的所有无理数.

4. 关注$\{x\}=x-[x]$性质的运用

例23 （第10届地中海地区数学竞赛题）设x为大于1的非整数. 证明：

$$\left(\frac{x+\{x\}}{[x]}-\frac{[x]}{x+\{x\}}\right)+\left(\frac{x+[x]}{\{x\}}-\frac{\{x\}}{x+[x]}\right)>\frac{9}{2},$$

其中，$[x]$与$\{x\}$分别表示x的整数部分和小数部分.

证明 设$[x]=a$，$\{x\}=r(0\leqslant r<1)$，则题中不等式等价于

$$\left(\frac{a+2r}{a}-\frac{a}{a+2r}\right)+\left(\frac{2a+r}{r}-\frac{r}{2a+r}\right)>\frac{9}{2}$$

$$\Leftrightarrow 2\left(\frac{r}{a}+\frac{a}{r}\right)-\left(\frac{a}{a+2r}+\frac{r}{2a+r}\right)>\frac{5}{2}.$$

由于$\frac{r}{a}+\frac{a}{r}\geqslant 2$，故只需证

$$\frac{a}{a+2r}+\frac{r}{2a+r}<\frac{3}{2}.$$

又$\frac{a}{a+2r}+\frac{r}{2a+r}<\frac{3}{2}\Leftrightarrow 0<2a^2+11ar+2r^2\Leftrightarrow 2(a+r)^2+7ar>0$.

显然成立.

综上所述，原不等式得证.

例24 （1990年国家集训队训练题）设$S(x)$表示数列$\{[nx]\}_{n\in\mathbf{N}}$，证明方程

$$x^3-10x^2+29x-25=0$$

有相异的两实根α,β，使$S(\alpha)\cap S(\beta)$中有无穷多个正整数.

证明 记$f(x)=x^3-10x^2+29x-25$，则

$f(1)=-5<0, f(2)=1>0$,

$f(2)=1>0, f(3)=-1>0$,

$f(5)=-5<0, f(6)=5>0$.

于是，方程 $f(x)=x^3-10x^2+29x-25=0$ 在区间 $(1,2),(2,3),(5,6)$ 中各有一根，设这三个实根为 α,β,γ，则

$$\alpha>0,\ \beta>0,\ \gamma>0,\ 且\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}=\frac{29}{25}.$$

若用 $S'(\alpha),S'(\beta),S'(\gamma)$ 表示 $S(\alpha),S(\beta),S(\gamma)$ 中小于或等于 M(M 为任意给定的自然数)的数的集合，则

$$|S'(\alpha)|=\left[\frac{M}{\alpha}\right],|S'(\beta)|=\left[\frac{M}{\beta}\right],|S'(\gamma)|=\left[\frac{M}{\gamma}\right],$$

$$\begin{aligned}&|S'(\alpha)\cap S'(\beta)|+|S'(\beta)\cap S'(\gamma)|+|S'(\alpha)\cap S'(\gamma)|\\ \geqslant&|S'(\alpha)|+|S'(\beta)|+|S'(\gamma)|-M\\ >&M\left(\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}-1\right)-3\\ >&\frac{4}{25}M-3.\end{aligned}$$

由此可得，当 M 趋向于无穷时，①式中的三项中必有一项趋于无穷．所以，必有满足方程的两实根（不妨设为 α，β），使 $S(\alpha)\cap S(\beta)$ 中有无穷多个自然数．

例 25　（1997 年第 26 届美国数学奥林匹克题）设 p_1，p_2，p_3，…是依递增次序排列的素数，x_0 是 0 与 1 之间的实数．对正整数 k，定义

$$x_k=\begin{cases}0, & 若\ x_{k-1}=0,\\ \left\{\dfrac{p_k}{x_{k-1}}\right\}, & 若\ x_{k-1}\neq 0.\end{cases}$$

这里 $\{x\}$ 表示 x 的小数部分．求出一切 x_0 满足 $0<x_0<1$ 且使数列 x_0，x_1，x_2，…中最终出现 0，并加以证明．

解　我们证明，该数列最终出现 0，当且仅当 x_0 为有理数．

首先，我们证明对 $k\geqslant1$，若 x_k 为有理数，则它的前一项 x_{k-1} 也是有理数．

若 $x_k=0$（为有理数），则由题设定义，或者有 $x_{k-1}=0$，或者有 $\dfrac{p_k}{x_{k-1}}$ 为正整数，从而 x_{k-1} 为有理数．

若 x_k 为非零有理数，那么由 $x_k=\left\{\dfrac{p_k}{x_{k-1}}\right\}=\dfrac{p_k}{x_{k-1}}-\left[\dfrac{p_k}{x_{k-1}}\right]$ 可得

$$x_{k-1}=\frac{p_k}{x_k+\left[\dfrac{p_k}{x_{k-1}}\right]},$$

于是 x_{k-1} 也是有理数．

由以上结论可知，对某个 k，若 x_k 是有理数，特别地，若数列最终出现 0，那么 x_0 也是有理数.

现设 x_0 为有理数，那么数列 $x_0,x_1,x_2,\cdots$ 为有理数列.

若 $x_{k-1}=\dfrac{m}{n}$，$0<m<n$，那么

$$x_k=\left\{\frac{p_k}{\frac{m}{n}}\right\}=\left\{\frac{n\cdot p_k}{m}\right\}=\frac{r}{m},0<r<m.$$

这里 r 是 np_k 除以 m 的余数.

所以，数列 $\{x_k\}$ 的每一个非零项的分母严格地小于前一项的分母，从而非零项的个数不超过 x_0 的分母.

因此，数列 $\{x_k\}$ 最终必出现 0.

例 26 （2005 年罗马尼亚数学奥林匹克题）已知方程 $\{x\{x\}\}=\alpha$，$\alpha\in(0,1)$.

(1) 证明：当且仅当 m，p，$q\in\mathbf{Z}$，$0<p<q$，p，q 互素，$\alpha=\left(\dfrac{p}{q}\right)^2+\dfrac{m}{q}$ 时，方程有有理数解.

(2) 当 $\alpha=\dfrac{2004}{2005^2}$ 时，求方程的一个解.

解 (1) 设 x 为所给方程的一个有理数解. 这意味着

$[x]=n$，$\{x\}=\dfrac{p}{q}$，其中，$0<p<q$，$n,p,q\in\mathbf{Z}$，p,q 互素.

设 $[x\{x\}]=k$，则有

$$\alpha=\left(n+\frac{p}{q}\right)\frac{p}{q}-k=\left(\frac{p}{q}\right)^2+\frac{m}{q}，其中，m=np-kq.$$

反之，设 $\alpha=\left(\dfrac{p}{q}\right)^2+\dfrac{m}{q}$.

因为 p,q 互素，则存在整数 a,b，使 $1=ap-bq$ 成立. 于是，有

$$\alpha=\frac{p^2+mq(ap-bq)}{q^2}=\left(ma+\frac{p}{q}\right)\frac{p}{q}-mb.$$

因此，方程有一个有理数解 $x=ma+\dfrac{p}{q}$.

(2) 寻找整数 p，m，使

$$\alpha=\frac{2004}{2005^2}=\left(\frac{p}{2005}\right)^2+\frac{m}{2005}，其中，0<p<2005，且(p,2005)=1.$$

该等式等价于

$$p^2+1=2005(1-m).$$

又 $2005=5\times401$，于是，有

$p^2\equiv-1(\bmod 5)$，$p^2\equiv-1(\bmod 401)$.

因为 $20^2\equiv 1(\bmod 401)$，当对某些整数 n 而言，$p=401n+20$ 时，条件 $p^2\equiv-1(\bmod 401)$成立.

当 $n^2\equiv-1(\bmod 5)$时，另一个条件得到满足，由此得 $n=2$，$p=822$.

由计算得有理数解为

$x=336\times822+\frac{822}{2005}$.

例 27 （第 35 届美国数学奥林匹克题）设 p 是一个素数，整数 s 满足：$0<s<p$. 证明：存在整数 m，n 满足 $0<m<n<p$ 及 $\left\{\frac{ms}{p}\right\}<\left\{\frac{ns}{p}\right\}<\frac{s}{p}$ 的充分必要条件是 s 不能整除 $p-1$.

证明 若 s 是 $p-1$ 的因数，设 $d=\frac{p-1}{s}$，于是，$(s,p,)=1$. 当 x 取遍 $1,2,\cdots,p-1$时，$\left\{\frac{sx}{p}\right\}$构成$\frac{1}{p},\frac{2}{p},\cdots,\frac{p-1}{p}$的一个排列.

显然，满足$\left\{\frac{sx}{p}\right\}<\frac{s}{p}$的值为$\frac{1}{p},\frac{2}{p},\cdots,\frac{s-1}{p}$.

又因为$\left\{\frac{sd}{p}\right\}=\frac{p-1}{p}$，且当 x 分别等于 $d,2d,\cdots,(s-1)d$ 时，$\left\{\frac{sx}{p}\right\}$分别等于$\frac{p-1}{p}$，$\frac{p-2}{p},\cdots,\frac{p-s+1}{p}$，所以，当 x 分别等于 $p-d,p-2d,\cdots,p-(s-1)d$ 时，$\left\{\frac{sx}{p}\right\}$分别等于$\frac{1}{p},\frac{2}{p},\cdots,\frac{s-1}{p}$.

因此，不存在整数 $m,n(0<m<n<p)$满足

$\left\{\frac{sm}{p}\right\}<\left\{\frac{sn}{p}\right\}<\frac{s}{p}$.

若 s 不是 $p-1$ 的因数，设 $m=\left[\frac{p}{s}\right]$（$[x]$表示大于 x 的最小整数），即$\frac{p}{s}<m<\frac{p}{s}+1$，有

$1<\frac{ms}{p}<1+\frac{s}{p}$，且$\left\{\frac{ms}{p}\right\}=\frac{ms-p}{p}<\frac{s}{p}$，

于是，m 是满足上式中最小的正整数.

若$\left\{\frac{ms}{p}\right\}=\frac{s-1}{p}$，则有$(m-1)s=p-1$，矛盾.

因此，存在 $n\in\{1,2,\cdots,p-1\}$，使得 $\left\{\frac{ns}{p}\right\}=\frac{s-1}{p}$，且 $n>m$.

注：满足 $\left\{\frac{ms}{p}\right\}<\frac{s}{p}$ 的最小的 m 应满足

$0<\frac{ms}{p}-\left[\frac{ms}{p}\right]<\frac{s}{p}$，即 $\frac{p}{s}\left[\frac{ms}{p}\right]<m<1+\frac{p}{s}\left[\frac{ms}{p}\right]$.

只有当 $\left[\frac{ms}{p}\right]=1$ 时，m 最小，此时有 $\frac{p}{s}<m<\frac{p}{s}+1$.

例 28 （2005 年全国高中数学联赛题）对每个正整数 n，定义函数

$$f(n)=\begin{cases}0, & \text{当 } n \text{ 为平方数,}\\ \left[\frac{1}{\{\sqrt{n}\}}\right], & \text{当 } n \text{ 不为平方数.}\end{cases}$$

（其中 $[x]$ 表示不超过 x 的最大整数，$\{x\}=x-[x]$）. 试求：$\sum_{k=1}^{240}f(k)$ 的值.

解法 1 对任意 a，$k\in\mathbf{N}_+$，若 $k^2<a<(k+1)^2$，设

$a=k^2+m$，$m=1, 2, \cdots, 2k$，

$\sqrt{a}=k+\theta$，$0<\theta<1$，

则

$$\left[\frac{1}{\{\sqrt{a}\}}\right]=\left[\frac{1}{\sqrt{a}-k}\right]=\left[\frac{\sqrt{a}+k}{a-k^2}\right]=\left[\frac{2k+\theta}{m}\right].$$

因为

$$0<\frac{2k+\theta}{m}-\frac{2k}{m}<1,$$

若在 $\frac{2k}{m}$ 与 $\frac{2k+\theta}{m}$ 之间存在整数 t，则 $\frac{2k}{m}<t<\frac{2k+\theta}{m}$.

于是，一方面，$2k<mt$，故 $2k+1\leqslant mt$，另一方面，$mt<2k+\theta<2k+1$，矛盾.

故 $\left[\frac{2k+\theta}{m}\right]=\left[\frac{2k}{m}\right]$，

所以 $$\sum_{k^2<a<(k+1)^2}\left[\frac{1}{\{a\}}\right]=\sum_{m=1}^{2k}\left[\frac{2k}{m}\right],$$

于是 $$\sum_{a=1}^{(n+1)^2}f(a)=\sum_{k=1}^{n}\sum_{i=1}^{2k}\left[\frac{2k}{i}\right]. \quad ①$$

下面计算 $\sum_{i=1}^{2k}\left[\frac{2k}{i}\right]$：画一张 $2k\times 2k$ 的表，第 i 行中，凡是 i 的倍数处填写“ * ”号，则这行的“ * ”号共 $\left[\frac{2k}{i}\right]$ 个，全表的“ * ”号共 $\sum_{i=1}^{2k}\left[\frac{2k}{i}\right]$ 个；另一方面，按列收集“ * ”号

数:第 j 列中,若 j 有 $T(j)$ 个正因数,则该列便有 $T(j)$ 个"*"号,故全表的"*"号个数共 $\sum_{j=1}^{2k} T(j)$ 个,因此 $\sum_{i=1}^{2k}\left[\frac{2k}{i}\right]=\sum_{j=1}^{2k} T(j)$.

示例如下:

i \ j	1	2	3	4	5	6
1	*	*	*	*	*	*
2		*		*		*
3			*			*
4				*		
5					*	
6						*

则

$$\begin{aligned}\sum_{a=1}^{(n+1)^2} f(a) &= \sum_{k=1}^{n}\sum_{j=1}^{2k} T(j)\\ &= n[T(1)+T(2)]+(n-1)[T(3)+T(4)]+\cdots+\\ &\quad [T(2n-1)+T(2n)].\end{aligned} \quad ②$$

由此 $$\sum_{k=1}^{16^2} f(k)=\sum_{k=1}^{15}(16-k)[T(2k-1)+T(2k)]. \quad ③$$

记 $a_k=T(2k-1)+T(2k)$, $k=1,2,\cdots,15$,易得 a_k 的取值情况如下:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_k	3	5	6	6	7	8	6	9	8	8	8	10	7	10	10

因此 $$\sum_{k=1}^{256} f(k)=\sum_{k=1}^{15}(16-k)a_k=783. \quad ④$$

由定义 $f(256)=f(16^2)=0$,当 $k\in\{241,242,\cdots,255\}$,设 $k=15^2+r(16\leqslant r\leqslant 30)$,

$$\sqrt{k}-15=\sqrt{15^2+r}-15=\frac{r}{\sqrt{15^2+r}+15},$$

$$\frac{r}{31}<\frac{r}{\sqrt{15^2+r}+15}<\frac{r}{30},$$

$$1\leqslant\frac{30}{r}<\frac{1}{\{\sqrt{15^2+r}\}}<\frac{31}{r}<2,$$

则 $\left[\frac{1}{\{\sqrt{k}\}}\right]=1, k\in\{241,242,\cdots,255\}$,

从而 $\sum\limits_{k=1}^{240}f(k)=783-\sum\limits_{k=1}^{256}f(k)=783-15=768.$

解法 2 $15^2<240<16^2$.

由于 k 为完全平方数时，$f(k)=0$,故

$$\sum_{k=1}^{240}f(k)=\sum_{k=1+1}^{2^2-1}f(k)+\sum_{k=2^2+1}^{3^2-1}f(k)+\cdots+\sum_{k=14^2+1}^{15^2-1}f(k)+\sum_{k=226}^{240}f(k)$$

$$=\sum_{n=1}^{14}\sum_{k=n^2+1}^{(n+1)^2-1}f(k)+\sum_{k=226}^{240}f(k).$$

当 $n^2+1\leqslant k\leqslant(n+1)^2-1$ 时，$[\sqrt{k}]=n$, $\{k\}=\sqrt{k}-[k]=\sqrt{k}-n$.

故 $\left[\frac{1}{\{\sqrt{k}\}}\right]=\left[\frac{1}{\sqrt{k}-n}\right]=\left[\frac{\sqrt{k}+n}{k-n^2}\right]=\left[\frac{[\sqrt{k}+n]}{k-n^2}\right]=\left[\frac{2n}{k-n^2}\right]$.

所以 $\sum\limits_{k=n^2+1}^{(n+1)^2-1}f(k)=\sum\limits_{k=n^2+1}^{(n+1)^2-1}\left[\frac{2n}{k-n^2}\right]=\sum\limits_{i=1}^{2n}\left[\frac{2n}{i}\right]$,

$$\sum_{k=226}^{240}f(k)=\sum_{k=226}^{240}\left[\frac{2\cdot 15}{k-15^2}\right]=\sum_{i=1}^{15}\left[\frac{30}{i}\right].$$

故 $\sum\limits_{k=1}^{240}f(k)=\sum\limits_{n=1}^{14}\sum\limits_{i=1}^{2n}\left[\frac{2n}{i}\right]+\sum\limits_{i=1}^{15}\left[\frac{30}{i}\right]$

$$=\sum_{n=1}^{14}\left(\sum_{i=1}^{n}\left[\frac{2n}{i}\right]+\sum_{i=n+1}^{2n}\left[\frac{2n}{i}\right]\right)+\sum_{i=1}^{15}\left[\frac{30}{i}\right]$$

$$=\sum_{n=1}^{14}\left(\sum_{i=1}^{n}\left[\frac{2n}{i}\right]+n\right)+\sum_{i=1}^{15}\left[\frac{30}{i}\right]$$

$$=\sum_{n=1}^{14}\sum_{i=1}^{n}\left[\frac{2n}{i}\right]+\sum_{i=1}^{15}\left[\frac{30}{i}\right]+\sum_{n=1}^{14}n$$

$$=\sum_{n=1}^{15}\sum_{i=1}^{n}\left[\frac{2n}{i}\right]+105.$$

设 $T_n=\sum\limits_{i=1}^{n}\left[\frac{2n}{i}\right], 1\leqslant n\leqslant 15$，则

$T_1=\left[\frac{2}{1}\right]=2, T_2=\left[\frac{4}{1}\right]+\left[\frac{4}{2}\right]=4+2=6$,

$T_3=\left[\frac{6}{1}\right]+\left[\frac{6}{2}\right]+\left[\frac{6}{3}\right]=6+3+2=11$,

$T_4=\left[\frac{8}{1}\right]+\left[\frac{8}{2}\right]+\left[\frac{8}{3}\right]+\left[\frac{8}{4}\right]=8+4+2\times 2=16$,

$T_5=\left[\frac{10}{1}\right]+\left[\frac{10}{2}\right]+\cdots+\left[\frac{10}{5}\right]=10+5+3+2\times2=22$,

$T_6=\left[\frac{12}{1}\right]+\left[\frac{12}{2}\right]+\cdots+\left[\frac{12}{6}\right]=12+6+4+3+2\times2=29$,

$T_7=\left[\frac{14}{1}\right]+\left[\frac{14}{2}\right]+\cdots+\left[\frac{14}{7}\right]=14+7+4+3+2\times3=34$,

$T_8=\left[\frac{16}{1}\right]+\left[\frac{16}{2}\right]+\cdots+\left[\frac{16}{8}\right]=16+8+5+4+3+2\times3=42$,

$T_9=\left[\frac{18}{1}\right]+\left[\frac{18}{2}\right]+\cdots+\left[\frac{18}{9}\right]=18+9+6+4+3\times2+2\times3=49$,

$T_{10}=\left[\frac{20}{1}\right]+\left[\frac{20}{2}\right]+\cdots+\left[\frac{20}{10}\right]=20+10+6+5+4+3+2\times4=56$,

$T_{11}=\left[\frac{22}{1}\right]+\left[\frac{22}{2}\right]+\cdots+\left[\frac{22}{11}\right]=22+11+7+5+4+3\times2+2\times4=63$,

$T_{12}=\left[\frac{24}{1}\right]+\left[\frac{24}{2}\right]+\cdots+\left[\frac{24}{12}\right]=24+12+8+6+4\times2+3\times2+2\times4=72$,

$T_{13}=\left[\frac{26}{1}\right]+\left[\frac{26}{2}\right]+\cdots+\left[\frac{26}{13}\right]=26+13+8+6+5+4+3\times2+2\times5=78$,

$T_{14}=\left[\frac{28}{1}\right]+\left[\frac{28}{2}\right]+\cdots+\left[\frac{28}{14}\right]=28+14+9+7+5+4\times2+3\times2+2\times5=87$,

$T_{15}=\left[\frac{30}{1}\right]+\left[\frac{30}{2}\right]+\cdots+\left[\frac{30}{15}\right]=30+15+10+7+6+5+4+3\times3+2\times5=96$.

故
$$\begin{aligned}\sum_{k=1}^{240}f(k)&=\sum_{n=1}^{15}T_n+105\\&=2+6+11+16+22+29+34+42+49+56+63+72+78+\\&\quad 87+96+105\\&=768.\end{aligned}$$

例 29 （2003 年全国高中数学联赛题）设三角形的三边长分别是整数 l，m，n，且 $l>m>n$. 已知 $\left\{\frac{3^l}{10^4}\right\}=\left\{\frac{3^m}{10^4}\right\}=\left\{\frac{3^n}{10^4}\right\}$，其中 $\{x\}=x-[x]$，而 $[x]$ 表示不超过 x 的最大整数. 求这种三角形周长的最小值.

解 由题设可知

$$\frac{3^l}{10^4}-\left[\frac{3^l}{10^4}\right]=\frac{3^m}{10^4}-\left[\frac{3^m}{10^4}\right]=\frac{3^n}{10^4}-\left[\frac{3^n}{10^4}\right].$$

于是 $3^l\equiv3^m\equiv3^n \pmod{10^4}$

$$\Leftrightarrow\begin{cases}3^l\equiv3^m\equiv3^n \pmod{2^4}, & ①\\ 3^l\equiv3^m\equiv3^n \pmod{5^4}. & ②\end{cases}$$

由于$(3,2)=1$，则由①可知

$3^{l-n}\equiv 3^{m-n}\equiv 1 \pmod{2^4}$.

设u是满足$3^u\equiv 1 \pmod{2^4}$的最小正整数，则对任意满足$3^v\equiv 1 \pmod{2^4}$的正整数v，有$u\mid v$，即u整除v．事实上，若$u\nmid v$，则由带余除法可知，存在非负整数a及b，使得$v=au+b$，其中$0<b\leqslant u-1$．从而，可推出$3^b\equiv 3^{b+au}\equiv 3^v\equiv 1 \pmod{2^4}$，而这显然与$u$的定义矛盾，所以，$u\mid v$.

注意到$3\equiv 3 \pmod{2^4}$，$3^2\equiv 9 \pmod{2^4}$，$3^3=27\equiv 11 \pmod{2^4}$，$3^4\equiv 1 \pmod{2^4}$，因此，$u=4$．从而，可设$m-n=4k$，其中$k$为正整数.

同理，可由②推出$3^{m-n}\equiv 1 \pmod{5^4}$，故$3^{4k}\equiv 1 \pmod{5^4}$.

下面求满足$3^{4k}\equiv 1 \pmod{5^4}$的正整数$k$.

因为$3^{4k}-1=(1+5\times 2^4)^k-1\equiv 0 \pmod{5^4}$，即

$$5k\times 2^4+\frac{k(k-1)}{2}\times 5^2\times 2^8+\frac{k(k-1)(k-2)}{6}\times 5^3\times 2^{12}$$

$$\equiv 5k+5^2k[3+(k-1)\times 2^7]+\frac{k(k-1)(k-2)}{3}\times 5^3\times 2^{11}$$

$$\equiv 0 \pmod{5^4},$$

所以$k=5t$，代入上式得

$t+5t[3+(5t-1)\times 2^7]\equiv 0 \pmod{5^2}$.

进而　$t\equiv 0 \pmod{5^2}$，

于是$k=5t=5^3s$，其中s为正整数，故$m-n=500s$，s为正整数.

同理可证$l-n=500r$，r为正整数.

由于$l>m>n$，所以$r>s$.

因此，三角形三边为$500r+n$，$500s+n$和n，且有$n>500(r-s)$．因此，当$s=1$，$r=2$，$n=501$时三角形周长最小，其值为

$(1000+501)+(500+501)+501=3\ 003$.

注：解决此题的一个关键是求出满足同余式$3^u\equiv 1 \pmod{10^4}$的最小整数，这个数在数论中定义为3对模10^4的指数（或阶）.

5. 发掘隐含条件，借助于函数$[x]$的性质解题

例30　（2004年全国高中数学联赛题）对于整数$n\geqslant 4$，求出最小的整数$f(n)$，使得对于任何正整数m，集合$\{m, m+1, \cdots, m+n-1\}$的任一个$f(n)$元子集中，均有至少3个两两互素的元素.

解法1　当$n\geqslant 4$时，考察集合$M=\{m, m+1, m+2, \cdots, m+n-1\}$.

若$2\mid m$，则$m+1$，$m+2$，$m+3$两两互素；

若$2\nmid m$，则m，$m+1$，$m+2$两两互素.

于是，M 的所有 n 元子集中，均有至少 3 个两两互素的元素. 因此，$f(n)$存在，且 $f(n)\leqslant n$.

设 $T_n=\{t\mid t\leqslant n+1$ 且 $2\mid t$ 或 $3\mid t\}$，则 T_n 为$\{2,3,\cdots,n+1\}$的子集，但 T_n 中任 3 个元素均不能两两互素，因此，$f(n)\geqslant|T_n|+1$.

由容斥原理知

$$|T_n|=\left[\frac{n+1}{2}\right]+\left[\frac{n+1}{3}\right]-\left[\frac{n+1}{6}\right],$$

从而必有

$$f(n)\geqslant\left[\frac{n+1}{2}\right]+\left[\frac{n+1}{3}\right]-\left[\frac{n+1}{6}\right]+1. \quad ①$$

因此　$f(4)\geqslant4,f(5)\geqslant5,f(6)\geqslant5,$

$f(7)\geqslant6,f(8)\geqslant7,f(9)\geqslant8.$

以下证明 $f(6)=5$.

设 x_1,x_2,x_3,x_4,x_5 为$\{m,m+1,\cdots,m+5\}$ 中的 5 个数. 若这 5 个数中有 3 个奇数，则它们两两互素；若这 5 个数中有 2 个奇数，则必有 3 个偶数，不妨设 x_1,x_2,x_3 为偶数，x_4,x_5 为奇数，当 $1\leqslant i<j\leqslant3$ 时，$|x_i-x_j|\in\{2,4\}$，所以 x_1,x_2,x_3 中至多一个被 3 整除，至多一个被 5 整除，从而至少有一个既不被 3 整除也不被 5 整除，不妨设 $3\nmid x_3,5\nmid x_3$，则 x_3,x_4,x_5 两两互素，这就是说这 5 个数中有 3 个两两互素，即 $f(6)=5$.

又由$\{m,m+1,\cdots,m+n\}=\{m,m+1,\cdots,m+n-1\}\cup\{m+n\}$知

$f(n+1)\leqslant f(n)+1.$

因为 $f(6)=5$，所以

$f(4)=4,f(5)=5,f(7)=6,f(8)=7,f(9)=8.$

因此，当 $4\leqslant n\leqslant9$ 时，

$$f(n)=\left[\frac{n+1}{2}\right]+\left[\frac{n+1}{3}\right]-\left[\frac{n+1}{6}\right]+1. \quad ②$$

以下用归纳法证明②对所有 n 都成立.

假设 $n\leqslant k$ ($k\geqslant9$) 时②式都成立.

当 $n=k+1$ 时，由于

$$\{m,m+1,\cdots,m+k\}=\{m,m+1,\cdots,m+k-6\}\cup\{m+k-5,m+k-4,m+k-3,m+k-2,m+k-1,m+k\},$$

且由归纳假设 $n=6$，$n=k-5$ 时，②式成立，所以

$$f(k+1)\leqslant f(k-5)+f(6)-1=\left[\frac{k+2}{2}\right]+\left[\frac{k+2}{3}\right]-\left[\frac{k+2}{6}\right]+1. \quad ③$$

由①，③式知，对于$n=k+1$，②式成立.

所以，对于任意$n\geqslant 4$，有

$$f(n)=\left[\frac{n+1}{2}\right]+\left[\frac{n+1}{3}\right]-\left[\frac{n+1}{6}\right]+1.$$

解法2 先验证$f(4)=4,f(5)=5,f(6)=5$.

$n=4$:$\{m,m+1,m+2,m+3\}$.若m为奇数,则$m,m+1,m+2$两两互素;若m为偶数,则$m+1,m+2,m+3$两两互素,故$f(4)\leqslant 4$.但在$\{m,m+1,m+2,m+3\}$中取二偶一奇的三元子集,此三数不能两两互素,故$f(4)=4$.

$n=5$:$\{m,m+1,m+2,m+3,m+4\}$.若m为偶数,则$m,m+2,m+4$均为偶数,则四元子集$\{m,m+1,m+2,m+4\}$中任三数不能两两互素,故$f(5)>4$,五元全集中可取到两两互素的三个数,故$f(5)=5$.

$n=6$:$\{m,m+1,m+2,m+3,m+4,m+5\}$中有三奇三偶,如果取三偶一奇的四元子集,则无三数两两互素,故$f(6)>4$，考察五元子集，若五元中有三个奇数，则此三数必两两互素；若五元中为三偶二奇，由于三个偶数中至多只有一个被3整除，至多只有一个被5整除，所以三个偶数中必有一个不被3整除，也不被5整除. 此数与其他两个奇数两两互素，故$f(6)=5$.

$n>6$:设$T_n=\{t:t\leqslant n+1,2|t$或$3|t\}$,则$T_n$为$\{2,3,\cdots,n+1\}$的子集. T_n中任三元素不能两两互素，所以

$$F(n)\geqslant|T_n|+1=\left[\frac{n+1}{2}\right]+\left[\frac{n+1}{3}\right]-\left[\frac{n+1}{6}\right]+1.$$

设$n=6k+r,k\geqslant 1,r=0,1,2,3,4,5$,则

$$\left[\frac{n+1}{2}\right]+\left[\frac{n+1}{3}\right]-\left[\frac{n+1}{6}\right]+1=4k+\left[\frac{r+1}{2}\right]+\left[\frac{r+1}{3}\right]-\left[\frac{r+1}{6}\right]+1.$$

易验证 $\left[\frac{r+1}{2}\right]+\left[\frac{r+1}{3}\right]-\left[\frac{r+1}{6}\right]=\begin{cases}r,r=0,1,2,3,\\ r-1,r=4,5.\end{cases}$

当$r=0，1，2，3$时，将$n=6k+r$个数按$\{m，m+1，\cdots，m+5\}$，$\{m+6，m+7，\cdots，m+11\}$，…，$\{m+6(k-1),m+6k-5,\cdots,m+6k-1\}$分成$k$组，并余下$r$个数$m+6k$，…，$m+6k+r-1$. $4k+r+1$个数中至少有$4k+1$个分在k个抽屉中，至少有一个抽屉中有五个数，由于$f(6)=5$，故必有三数两两互素.

当$r=4，5$时，可以类似证明，必有三数两两互素.

故$f(n)=\left[\frac{n+1}{2}\right]+\left[\frac{n+1}{3}\right]-\left[\frac{n+1}{6}\right]+1.$

例31 （2003年白俄罗斯数学奥林匹克题）问是否存在一个满射的函数f，f：$\mathbf{R}\to\mathbf{R}$，使得对于任意实数x和y，$f(x+y)-f(x)-f(y)$的取值只有两个数:0和1.

解 函数 $f(x)=\frac{1}{2}([x]-\{x\})$ 满足条件，其中 $[x]$ 表示不超过 x 的最大整数，$\{x\}=x-[x]$.

对于所有实数 x,y，

$x=[x]+\{x\}, y=[y]+\{y\}$.

下面分两种情况证明.

若 $0\leqslant\{x\}+\{y\}<1$，则

$x+y=[x]+\{x\}+[y]+\{y\}=([x]+[y])+(\{x\}+\{y\})$.

因为 $0\leqslant\{x\}+\{y\}-1<1$，所以

$\{x+y\}=[x]+[y], \{x+y\}=\{x\}+\{y\}$.

于是有

$$
\begin{aligned}
& f(x+y)-f(x)-f(y) \\
=& \frac{1}{2}([x]+[y]-\{x\}-\{y\}-[x]+\{x\}-[y]+\{y\}) \\
=& 0.
\end{aligned}
$$

若 $1\leqslant\{x\}+\{y\}<2$，则

$x+y=([x]+[y]+1)+(\{x\}+\{y\}-1)$.

因为 $0\leqslant\{x\}+\{y\}-1<1$，所以

$[x+y]=[x]+[y]+1$,

$\{x+y\}=\{x\}+\{y\}-1$.

于是有

$$
\begin{aligned}
& f(x+y)-f(x)-f(y) \\
=& \frac{1}{2}([x]+[y]+1-\{x\}-\{y\}+1-[x]+\{x\}-[y]+\{y\})=1.
\end{aligned}
$$

下面证明 $f: \mathbf{R}\to\mathbf{R}$ 是满射.

对于任意实数 a，设 n 是满足 $2a\leqslant n$ 的最小的一个整数. 设 $\alpha=n-2a$，则 $0\leqslant\alpha<1$. 令 $x=n+\alpha$，则 $[x]=n$，$\{x\}=\alpha$，且 $[x]-\{x\}=n-\alpha=2a$，即存在 $x\in\mathbf{R}$，使得 $f(x)=a$.

所以，$f(x)=\frac{1}{2}([x]-\{x\})$ 是满射.

例 32 （CMO 6 试题）求所有的自然数 n，使得 $\min\limits_{k\in\mathbf{N}}\left(k^2+\left[\frac{n}{k^2}\right]\right)=1991$，这里 $\mathbf{N}$ 是自然数集.

解 由于

$$k^2+\frac{n}{k^2}-1<k^2+\left[\frac{n}{k^2}\right]\leqslant k^2+\frac{n}{k^2},$$

则$\min\limits_{k\in\mathbf{N}}\left(k^2+\left[\frac{n}{k^2}\right]\right)=1991$,

等价于:

对所有的 $k\in\mathbf{N}$,

$$k^2+\frac{n}{k^2}\geqslant 1991, \qquad ①$$

且存在 $k_0\in\mathbf{N}$,使得

$$k_0^2+\frac{n}{k_0^2}<1992. \qquad ②$$

由于①有

$k^4-1991k^2+n\geqslant 0$,

$\left(k^2-\frac{1991}{2}\right)^2+n-\frac{1991^2}{4}\geqslant 0$,

$n\geqslant\frac{1991^2}{4}-\left(k^2-\frac{1991}{2}\right)^2$.

为使此式成立,只要$\frac{1991^2}{4}-\left(k^2-\frac{1991}{2}\right)^2$的最大值小于或等于 n 即可.

由于最接近$\frac{1991}{2}$的平方数为 $32^2=1024$,所以当 $k=32$ 时,$\left(k^2-\frac{1991}{2}\right)^2$ 有最小值$\left(1024-\frac{1991}{2}\right)^2$.

从而有

$n\geqslant\frac{1991^2}{4}-\left(1024-\frac{1991}{2}\right)^2=967\cdot 1024$.

由于②,存在 $k_0\in\mathbf{N}$,使得

$k_0^4-1992k_0^2+n<0$,

$-(k_0^2-996)^2-n+996^2>0$,

$n<-(k_0^2-996)^2+996^2$.

为使此式成立,只要求出使$-(k_0^2-996)^2+996^2$ 的最大值大于 n 的 k_0 的值即可.

显然,$k_0=32$ 时,$-(k_0^2-996)^2+996$ 有最大值$-(1024-996)^2+996^2$,即

$n<-(1024-996)^2+996^2=1024\cdot 968$.

于是 $1024\cdot 967\leqslant n<1024\cdot 968$.

即集合$\{n\mid 1024\cdot 967\leqslant n<1024\cdot 968,n\in\mathbf{N}\}$为所求.

例 33 (2005 年国家集训队选拔考试题) 给定正整数 n ($n\geqslant 2$),求最大的 λ,

使得：若有 n 个袋子，每一个袋子中都有一些重量为 2 的整数次幂的小球，且各个袋子中的小球的总重量都相等，则必有某一重量的小球的总个数至少为 λ.（同一个袋子中可以有相等重量的小球）

解 不妨设最重的小球的重量为 1. 我们首先证明，$\lambda_{\max}\geqslant\left[\frac{n}{2}\right]+1$.

设每个袋子中小球的总重量为 G，则 $G\geqslant1$. 假设任一重量的小球的总个数都不大于 $\left[\frac{n}{2}\right]$，则由两方面考虑 n 个袋子中所有小球的总重量，得出

$$n\leqslant nG\leqslant\left[\frac{n}{2}\right]\left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots\right)<2\left[\frac{n}{2}\right]\leqslant n.$$

矛盾. 因此所说的断言成立.

另一方面，取充分大的整数 k，使得

$$2-2^{-k}\geqslant\frac{2n}{n+1},$$

则由于 $\left[\frac{n}{2}\right]+1\geqslant\frac{n+1}{2}$，故

$$2-2^{-k}\geqslant\frac{2n}{n+1}\geqslant\frac{n}{\left[\frac{n}{2}\right]+1},$$

从而

$$\left(\left[\frac{n}{2}\right]+1\right)\left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^k}\right)\geqslant n\times1.$$

因此，可在

$$\underbrace{1,1,\cdots,1}_{\left(\left[\frac{n}{2}\right]+1\right)个},\underbrace{\frac{1}{2},\frac{1}{2},\cdots,\frac{1}{2}}_{\left(\left[\frac{n}{2}\right]+1\right)个},\cdots,\underbrace{\frac{1}{2^k},\frac{1}{2^k},\cdots,\frac{1}{2^k}}_{\left(\left[\frac{n}{2}\right]+1\right)个}$$

中，由前至后依次取和为 1 的连续若干项，且至少可取 n 次. 故 $\lambda_{\max}\leqslant\left[\frac{n}{2}\right]+1$.

综合上述两个方面，得 $\lambda_{\max}=\left[\frac{n}{2}\right]+1$.

例 34 （2006 年国家集训队选拔考试题）给定正整数 m、a、b，$(a,b)=1$. A 是正整数集的非空子集，使得对任意的正整数 n 都有 $an\in A$ 或 $bn\in A$. 对所有满足上述性质的集合 A，求 $|A\cap\{1,2,\cdots,m\}|$ 的最小值.

解 (1) 当 $a=b=1$ 时，$A\cap\{1,2,\cdots,m\}=\{1,2,\cdots,m\}$，故 $|A\cap\{1,2,\cdots,m\}|=m$.

(2) 设 a，b 不全为 1，不妨设 $a>b$. 令

$A_1=\{k\mid 若\ a^l\mid k,a^{l+1}\nmid k,则\ l\ 是奇数\}$.

现验证 A_1 满足问题中的要求.

任取正整数 n,设 $n=a^l n_1$,a 不整除 n_1,当 $2|l$ 时,则有 $an=a^{l+1}n_1\in A_1$;若 $2\nmid l$,由于$(a,b)=1$,故 $bn=a^l bn_1\in A_1$.

此外,由于不超过 m,且被 a^i 整除的数共有$\left[\frac{m}{a^i}\right]$个,故由容斥原理易知

$$|A\cap\{1,2,\cdots,m\}|=\sum_{i=1}^{\infty}(-1)^{i+1}\left[\frac{m}{a^i}\right].$$

现在我们证明,当 $a>b$ 时,对任意具有问题中性质的 A,总有

$$|A\cap\{1,2,\cdots,m\}|\geqslant\sum_{i=1}^{\infty}(-1)^{i+1}\left[\frac{m}{a^i}\right].$$

为了证明,考虑二元子集:

$S_k=\{ak,bk\}$,其中 $k\leqslant\frac{m}{a}$,且 k 中所含 a 的幂次为偶数(即若 $a^l|k$,但 $a^{l+1}\nmid k$,则 l 为偶数).

由于$(a,b)=1$,故易知 $S_k\neq S_{k'}$(其中 k'具有与 k 相同的性质).此外,因 $a>b$,故 $1\leqslant ak,bk\leqslant m$,于是 ak,bk 中必有一个属于 A.若设上述二元子集 S_k 共有 S 个,则

$$|A\cap\{1,2,\cdots,m\}|\geqslant S=\sum_{i=1}^{\infty}(-1)^{i+1}\left[\frac{m}{a^i}\right].$$

(最后一步仍用容斥原理.)

综合上述结果可知,所求的最小值为 m(当 $a=b=1$ 时),得 $\sum_{i=1}^{\infty}(-1)^{i+1}\left[\frac{m}{c^i}\right]$[当 a,b 不全为 1 时,这里 $c=\max(a,b)$].

【模拟实战】

1. (1993 年全国高中数学联赛题) 整数$\left[\frac{10^{93}}{10^{31}+3}\right]$的末尾两位数字是多少?(先写十位数字,后写个位数字)

2. (1986 年第 1 届中国东北三省数学邀请赛题) 计算和式 $\sum_{n=0}^{502}\left[\frac{305n}{503}\right]$之值.

3. (1990 年第 1 届"希望杯"数学竞赛题) 求$\left[\frac{2+\sqrt{2}}{2}\right]+\left[\frac{3+\sqrt{3}}{3}\right]+\left[\frac{4+\sqrt{4}}{4}\right]+\cdots+\left[\frac{1989+\sqrt{1989}}{1989}\right]+\left[\frac{1990+\sqrt{1990}}{1990}\right]$.

4. (1990 年第 1 届"希望杯"数学竞赛题)求$[\sqrt{1}]+[\sqrt{2}]+[\sqrt{3}]+\cdots+[\sqrt{1989\cdot1990}]+[-\sqrt{1}]+[-\sqrt{2}]+[-\sqrt{3}]+\cdots+[-\sqrt{1989\cdot1990}]$的值等于多少?

5. (1948年第8届美国普特南数学竞赛题)如果 n 为一正整数,试证 $[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+2}]$.

6. (1988年理科实验班入学数学复试题) 设 $S=[\sqrt{1}]+[\sqrt{2}]+\cdots+[\sqrt{1988}]$,求 $[\sqrt{S}]$.

7. (1991年北京市数学竞赛题) 能使 $\left[\frac{n^2}{5}\right]$ 为素数的所有自然数 n 的倒数之和等于多少?

8. (1990年匈牙利数学奥林匹克题) 求方程 $[x^2-2x]=[x]^2-2[x]$ 的实数解.

9. (1991年前苏联教委[illegible]试[illegible] 解方程 $[x]\{x\}+x=2\{x\}+10$.

10. (1991年第2届"希望杯"[illegible]学竞赛题) 设 $\{x\}$ 表示不小于实数 x 的最小整数,则 $\{\log_2 1\}+\{\log_2 2\}+\{\log_2 3\}+\cdots+\{\log_2 1991\}$ 的值等于多少?

11. (1980年第6届全俄数学奥林匹克题) 在数列 $\left[\frac{1^2}{1980}\right],\left[\frac{2^2}{1980}\right],\left[\frac{3^2}{1980}\right],\cdots,\left[\frac{1980^2}{1980}\right]$ 中,有多少个不同的数?

12. (2004年国家队培训题) 对于所有素数 p 和所有正整数 n $(n\geqslant p)$ 证明: $C_n^p-\left[\frac{n}{p}\right]$ 能被 p 整除.

13. (IMO-47预选题) 已知数列 $f(1),f(2),\cdots$ 被定义为:

$$f(n)=\frac{1}{n}\left(\left[\frac{n}{1}\right]+\left[\frac{n}{2}\right]+\cdots+\left[\frac{n}{n}\right]\right),$$

其中,$[x]$ 表示不大于 x 的最大整数.证明:

(1) 有无穷多个 n,使得 $f(n+1)>f(n)$;

(2) 有无穷多个 n,使得 $f(n+1)<f(n)$.

14. (1981年第13届加拿大数学竞赛题) 试证方程

$$[x]+[2x]+[4x]+[8x]+[16x]+[32x]=12345$$

没有实数解.

15. (1991年四川省高中数学联赛题) 设正实数 $a>1$,自然数 $n\geqslant 2$,且方程 $[ax]=x$ 恰有 n 个不同的解.试求 a 的取值范围.

16. 设正实数 x,y 满足 $xy=1$,求函数

$$f(x,y)=\frac{x+y}{[x][y]+[x]+[y]+1}$$

的值域(其中 $[x]$ 表示不超过 x 的最大整数).

第十六章 整数的 p 进位制及应用

【基础知识】

给定一个 m 位正整数 A，其各位上的数字分别记为 a_{m-1}，a_{m-2}，…，a_0，此数可简记为 $A=\overline{a_{m-1}a_{m-2}\cdots a_0}$（其中 $a_{m-1}\neq 0$）.

由于我们所研究的整数通常是十进位制的，因此常将正整数 A 表示成关于 10 的 $m-1$次多项式，即

$$A=a_{m-1}\cdot 10^{m-1}+a_{m-2}\cdot 10^{m-2}+\cdots+a_1\cdot 10+a_0,$$

其中 $a_i\in\{0,1,2,\cdots,9\}$，$i=1,2,\cdots,m-1$，$a_{m-1}\neq 0$.

如上 10 的多项式表示的数常简记为 $A=(a_{m-1}a_{m-2}\cdots a_0)_{10}$.

在我们的课本中及常见到的各种资料中，通常将下足码 10 省略不写，括号也不打上（这与以 10 为底的对数一样处理）.

随着计算机的迅速普及，整数的表示除用到十进位制外，二进位制、八进位制等 p 进位制的记数法已被广泛采用. 更一般，我们给出正整数的 p 进位制表示：

给定一个自然数 p（p 进位制的基），可将任一正整数 A 唯一地表示成下述形式：

$A=a_{m-1}\cdot p^{m-1}+a_{m-2}\cdot p^{m-2}+\cdots+a_1\cdot p+a_0$，其中 $a_i\in\{0,1,2,\cdots,p-1\}$，$i=1,2,\cdots,m-1$，$a_{m-1}\neq 0$，而 m 为十进位制数.

这种 p 的多项式表示的数常简记为 $A=(a_{m-1}a_{m-2}\cdots a_0)_p$.

如何将一个正整数进行各种进位制的互化呢？我们看一个具体的例子.

将十进位制的 2004（如果没有指明进位制，则认为是十进位制省略了）化为二进位制的数和八进位制的数.

用 2 作除数（化 p 进位制就以 p 作除数），除 2004 商 1002，余数为 0；再用 2 除 1002，商 501，余数为 0；继续下去，直到商为 0 止. 所得的各次余数从左到右排列出来，便得到所化出的二进位制的数.

各次商数 ←											被除数	除数
0	1	3	7	15	31	62	125	250	501	1002	2004	2
	1	1	1	1	1	0	1	0	1	0	0	
各次余数 ←												

故$(2004)_{10}=(1\,1\,1\,1\,1\,0\,1\,0\,1\,0\,0)_2$，

$2\cdot10^4+4=1\cdot2^{10}+1\cdot2^9+1\cdot2^8+1\cdot2^7+1\cdot2^6+1\cdot2^4+1\cdot2^2$.

同样，有$(2004)_{10}=(3\,7\,2\,4)_8$，

$2\cdot10^4+4=3\cdot8^3+7\cdot8^2+2\cdot8+4$.

【典型例题与基本方法】

例1 （1979年云南省数学竞赛题）一个四位数，它的个位数字与百位数字相同，如果把这个四位数的数字顺序颠倒过来（即千位数字与个位数字互换，百位数字与十位数字互换），所得的新数减去原数得7812，求原来的四位数.

解 设该数的千位、百位、十位数字分别为x，y，z，则

原数$=10^3\cdot x+10^2\cdot y+10\cdot z+y$， ①

颠倒后的新数$=10^3\cdot y+10^2\cdot z+10y+x$. ②

②－①得 $7812=999(y-x)+90(z-y)$，

即 $868=111(y-x)+10(z-y)$

$=10^2\cdot(y-x)+10\cdot(z-x)+(y-x)$. ③

比较③式两端百位、十位、个位数字得

$y-x=8$，$z-x=6$.

原数千位数字x不能为零，所以$x\geqslant1$. 而$y=x+8\geqslant9$，又显见百位数字$y\leqslant9$，所以$y=9$，$x=1$，$z=x+6=7$.

故所求四位数是1979.

例2 （第3届加拿大数学竞赛题）设n是五位数（第一位数码不是零），m是由n取消它的中间一位数码后所成的四位数. 试确定一切n使得$\frac{n}{m}$是整数.

解 设$n=\overline{xyzuv}=x\cdot10^4+y\cdot10^3+z\cdot10^2+u\cdot10+v$，其中$x$，$y$，$z$，$u$，$v$是数码0，1，2，…，8或9中的一个，且$x\geqslant1$.

$m=\overline{xyuv}=x\cdot10^3+y\cdot10^2+u\cdot10+v$.

而$k=\frac{n}{m}$是整数. 可证不等式$9m<n$，即

$9\cdot(x\cdot10^3+y\cdot10^2+u\cdot10+v)<x\cdot10^4+y\cdot10^3+z\cdot10^2+u\cdot10+v$，

也就是 $80u+8v<10^3\cdot x+10^2\cdot y+10^2\cdot z$，这显然是正确的.

又可证不等式$n<11m$，即

$x\cdot10^4+y\cdot10^3+z\cdot10^2+u\cdot10+v<11\cdot(x\cdot10^3+y\cdot10^2+u\cdot10+v)$，

也就是$10^2\cdot z<10^3x+10^2y+10^2u+10v$，这显然是正确的.

于是，$9m<n<11m$，即$9<k<11$. 又因为k是整数，从而$k=10$.

于是，$n=10m$，即

$x\cdot 10^4+y\cdot 10^3+z\cdot 10^2+u\cdot 10+v=10(x\cdot 10^3+y\cdot 10^2+u\cdot 10+v)$，

亦即　$z\cdot 10^2=90\cdot u+9\cdot v=9(10u+v)$.

而由 9 整除 $z\cdot 10^2$，但 3 不能整除 10^2，知

$z=9t$（t 为整数），从而 $t\cdot 10^2=10u+v$.

显然，$t=u=v=0$.

因而，推得 $n=\overline{xy000}=N\cdot 10^3$，其中 $10\leqslant N\leqslant 99$.

例 3　（1994 年湖南省数学夏令营试题）N 是一个完全平方数，各位数均小于 7，且每一个数字增加 3 后仍是一个完全平方数．求这样的数 N.

解　设 $N=a_{2k-1}\cdot 10^{2k-1}+a_{2k-2}\cdot 10^{2k-2}+\cdots+a_1\cdot 10+a_0$，其中 $a_i(i=0,1,\cdots,2k-1$ 且 $k\in\mathbf{N})$ 是不大于 7 的非负整数，且 $a_{2k-1}\neq 0$.

由题设 $N=n^2$（n 为某正整数），则

$n^2\leqslant\underbrace{66\cdots6}_{2k个}$，

故 $n<82\underbrace{00\cdots0}_{k-2个}$.

又 $(a_{2k-1}+3)\cdot 10^{2k-1}+(a_{2k-2}+3)\cdot 10^{2k-2}+\cdots+(a_0+3)=m^2$（$m$ 是某正整数），

于是 $m^2-n^2=\underbrace{33\cdots3}_{2k个}$，即

$(m+n)(m-n)=3\cdot\underbrace{11\cdots1}_{k个}\cdot 1\underbrace{0\cdots0}_{k-1个}1$.

因 $m+n>m-n$，且 $n<82\underbrace{0\cdots0}_{k-2个}$，

故 $m+n=1\underbrace{0\cdots0}_{k-1个}1$ 且 $m-n=\underbrace{3\cdots3}_{k个}$.

因此 $n=\underbrace{3\cdots3}_{k-1个}4$.

故 $N=1$ 及 $N=\underbrace{11\cdots1}_{k个}\underbrace{55\cdots5}_{2k个}6$（$k\in\mathbf{N}$）为所求.

例 4　（第 32 届美国中学生数学竞赛题）在三进位制中，数 x 的表示是：12112211122211112222，则 x 在九进位制中表示式最左边一位是什么数？

解　把 x 的三进位制表示的数字一对对地组合，得到

$$\begin{aligned}x&=(1\cdot 3^{19}+2\cdot 3^{18})+(1\cdot 3^{17}+1\cdot 3^{16})+\cdots+(2\cdot 3+2)\\&=(1\cdot 3+2)\cdot(3^2)^9+(1\cdot 3+2)\cdot(3^2)^8+\cdots+(2\cdot 3+2).\end{aligned}$$

因此，x 的九进位制的第一位数字是 $1\cdot 3+2=5$.

例 5　（第 4 届美国数学邀请赛试题）递增数列 1，3，4，9，10，12，13，…由

一些正整数组成，它们或是 3 的幂，或是若干个不同的 3 的幂之和，求此数列的第 100 项.

解 将已知数列写成 3 的方幂和形式

$a_1=3^0$，$a_2=3^1$，$a_3=3^1+3^0$，$a_4=3^2$，$a_5=3^2+3^0$，$a_6=3^2+3^1$，

$a_7=3^2+3^1+3^0$，…

易发现其项数恰好是自然数列的对应形式的二进制表示：

$1=2^0$，$2=2^1$，$3=2^1+2^0$，$4=2^2$，$5=2^2+2^0$，$6=2^2+2^1$，

$7=2^2+2^1+2^0$，…

由于 $100=(1100100)_2=2^6+2^5+2^2$，

所以原数列的第 100 项为 $3^6+3^5+3^2=981$.

例 6 （1987 年加拿大数学竞赛题）1987 可以在 b 进制中写成三位数$\overline{xyz}$，如果 $x+y+z=1+9+8+7$，试确定所有可能的 x，y，z 和 b.

解 易知 $xb^2+yb+z=1987$，$x+y+z=25$，从而，

$x(b^2-1)+y(b-1)=1962$，即

$(b-1)[(b+1)x+y]=1962=2\times3^2\times109$.

由 $b>10$ 知 $b-1>9$；由 $1962\geqslant b^2-1$ 知 $b\leqslant\sqrt{1963}<45$.

故 $9<b-1<44$.

由 $1962=2\times3^2\times109$ 知它有 12 个正约数，分别为

1，2，3，6，9，18，109，218，327，654，981，1962.

所以，$b-1=18$，$b=19$.

由 $1987=5\times19^2+9\times19+11$ 知 $x=5$，$y=9$，$z=11$.

例 7 数列 $\{x_n\}$ 定义如下：$x_1=1$，对 $k>0$，

$$x_{2k}=\begin{cases}2x_k，若 k 为偶数,\\ 2x_k+1，若 k 为奇数;\end{cases}\quad x_{2k+1}=\begin{cases}2x_k，若 k 为奇数,\\ 2x_k+1，若 k 为偶数.\end{cases}$$

求证：数列 $\{x_n\}$ 能取遍每个正整数且恰好一次.

证明 全部用二进制表示数，令 $n=(\overline{a_ma_{m-1}\cdots a_1a_0})_2$. 下面用数学归纳法证明：$x_n=(\overline{b_mb_{m-1}\cdots b_1b_0})_2$，其中，$b_m=a_m=1$，$b_i\equiv a_i+a_{i+1}\pmod 2$，$i=0,1,2,\cdots,m-1$.

当 $n=1$ 时命题显然成立. 设对小于 n 的自然数命题成立. 对于 $n=(\overline{a_m\cdots a_1a_0})_2$，记 $n'=(\overline{a_m\cdots a_1})_2$，由题设

(1) 若 $a_1a_0=00$，则 $x_n=2x_{n'}=2\cdot(\overline{b_m\cdots b_1})_2=(\overline{b_m\cdots b_1b_0})_2$；

(2) 若 $a_1a_0=10$，则 $x_n=2x_{n'}+1=(\overline{b_m\cdots b_11})_2=(\overline{b_m\cdots b_1b_0})_2$；

(3) 若 $a_1a_0=01$，则 $x_n=2x_{n'}+1=(\overline{b_m\cdots b_11})_2=(\overline{b_m\cdots b_1b_0})_2$；

(4) 若 $a_1a_0=11$，则 $x_n=2x_{n'}=(\overline{b_m\cdots b_10})_2=(\overline{b_m\cdots b_1b_0})_2$.

从而知命题对 n 也成立.

若 $x_n=(\overline{b_m\cdots b_1b_0})_2$，则对任意数 $(\overline{b_mb_{m-1}\cdots b_1b_0})_2$，可以唯一确定 $n=(\overline{a_ma_{m-1}\cdots a_1a_0})_2$ 如下：

$a_m=b_m=1$，且 $a_i\equiv b_i-a_{i+1}\pmod 2$.

所以，$n\to x_n$，为 $N\to N$ 的一一对应，从而命题得证.

例 8 （第 19 届美国数学奥林匹克题）试求出并证明所有这样的正整数的个数：它在 n 进位制的表示中数字各不相同，并且除去最左边的数字，每一个数字均和它左边的某个数字相差 ±1（答案用 n 的显函数以最简单的形式表达）.

解法 1 考察具有题设要求性质的 n 进制中的 k 位数的个数.

显然这个 k 位数应该由 k 个连续的 n 进位数字组成，为此有如下结论：

(1) 对每个 $k=1,2,\cdots,n$ 有 $n-k+1$ 个可能的 k 个连续的 n 进位数字的集合：

$\{0,1,\cdots,k-1\},\{1,2,\cdots,k\},\cdots,\{n-k,n-k+1,\cdots,n-1\}$.

(2) 对于给定的 k 个连续数字，符合条件的排列方法有 2^{k-1} 种.

这是因为，最右边的或是各数字中最大的或是最小的，从右数第二个数字是剩下的数字中最大的或最小的，……，最左边的数字则为选定 $k-1$ 个数字之后剩下的数字.

(3) 对每个 k，恰有一个以 0 开头的 k 个连续数字的排列，这个数不是真正的 k 位数.

因此，由 (1)，(2)，(3)，满足要求的 k 位整数有 $(n-k+1)2^{k-1}-1$ 个.

当 $k=1,2,\cdots,n$ 时，对所有的 k 求和

$$
\begin{aligned}
&\sum_{k=1}^{n}[(n-k+1)\cdot 2^{k-1}-1]\\
&=[(\underbrace{2^0+2^0+\cdots+2^0}_{n个})-1]+[(\underbrace{2^1+2^1+\cdots+2^1}_{n-1个})-1]+\cdots+\\
&\quad[(2^{n-2}+2^{n-2})-1]+(2^{n-1}-1)\\
&=[(2^n-1)+(2^{n-1}-1)+\cdots+(2^2-1)+(2^1-1)]-n\\
&=[(2^n+2^{n-1}+\cdots+2^2+2^1)-n]-n\\
&=2^{n+1}-2n-2.
\end{aligned}
$$

解法 2 因为只有 0 不能作第一个数字，我们先定义 $F(n)$ 为 n 进位满足题设条件的整数，而先不考虑第一个数字是否为 0，则

$F(1)=1,\{0\}$,

$F(2)=4,\{0,01,1,10\}$,

$F(3)=11$, $\{0,01,012,1,10,102,12,120,2,21,210\}$.

现在建立 $F(n+1)$ 的递推式.

注意到 $n+1$ 进位中的数字串有三类:

(i) 单一的数字: 0, 1, 2, …, n;

(ii) 一个适当的 n 进位数字串, 接一个紧挨着最大的未用数字;

(iii) 一个适当的 n 进位数字串, 接一个紧挨着最小的未用数字.

于是有 $F(n+1)=n+1+2F(n)$, $F(1)=1$.

由此推得 $F(n)=2^{n+1}-n-2$.

由于以 0 作为第一个数字的数不合要求, 而这样的数, 在 n 进制中有 n 个, 即 0, 01, …, 012…$(n-1)$.

所以所求正整数的个数为 $F(n)-n=2^{n+1}-2n-2$.

例 9 (1999 年全国高中数学联赛题) 给定正整数 n, 已知用克数都是正整数的 k 块砝码和一台天平可以称出质量为 1, 2, 3, …, n 克的所有物品.

(1) 求 k 的最小值 $f(n)$;

(2) 当且仅当 n 取什么值时, 上述 $f(n)$ 块砝码的组成方式是唯一确定的? 并证明你的结论.

解 (1) 设这 k 块砝码的质量数分别为 a_1, a_2, …, a_k, 且 $1\leqslant a_1\leqslant a_2\leqslant\cdots\leqslant a_k$, $a_i\in\mathbf{Z}$, $1\leqslant i\leqslant k$. 因为天平两端都可以放砝码, 故可称质量为 $\sum\limits_{i=1}^{k}x_ia_i$, $x_i\in\{-1,0,1\}$. 若利用这 k 块砝码可以称出质量为 1, 2, 3, …, n 的物品, 则上述表示式中含有 1, 2, …, n, 由对称性易知也含有 0, -1, -2, …, $-n$, 即

$$\left\{\sum_{i=1}^{k}x_ia_i \mid x_i\in\{-1,0,1\}\right\}\supseteq\{0,\pm1,\cdots,\pm n\}.$$

所以, $2n+1=|\{0,\pm1,\cdots,\pm n\}|\leqslant\left|\left\{\sum\limits_{i=1}^{k}x_ia_i \mid x_i\in\{-1,0,1\}\right\}\right|\leqslant 3^k$,

即 $n\leqslant\dfrac{3^k-1}{2}$.

设 $\dfrac{3^{m-1}-1}{2}<n\leqslant\dfrac{3^m-1}{2}$ $(m\geqslant1, m\in\mathbf{Z})$, 则 $k\geqslant m$,

且 $k=m$ 时, 可取 $a_1=1$, $a_2=3$, …, $a_m=3^{m-1}$.

由数的三进制表示可知, 对任意 $0\leqslant p\leqslant 3^m-1$, 都有

$$p=\sum_{i=1}^{m}y_i3^{i-1}, \text{其中 } y_i\in\{0,1,2\}.$$

则 $$p-\frac{3^m-1}{2}=\sum_{i=1}^{m}y_i3^{i-1}-\sum_{i=1}^{m}3^{i-1}=\sum_{i=1}^{m}(y_i-1)3^{i-1}.$$

令 $x_i=y_i-1$，则 $x_i\in\{-1,0,1\}$.

故对一切 $-\frac{3^m-1}{2}\leqslant l\leqslant\frac{3^m-1}{2}$ 的整数 l，都有

$l=\sum_{i=1}^{m}x_i3^{i-1}$，其中 $x_i\in\{-1,0,1\}$.

由于 $n\leqslant\frac{3^m-1}{2}$，因此，对一切 $-n\leqslant l\leqslant n$ 的整数 l，也有上述表示.

综上，可知 k 的最小值 $f(n)=m$.（$\frac{3^{m-1}-1}{2}<n\leqslant\frac{3^m-1}{2}$）

(2) 首先，当 $\frac{3^m-1}{2}<n<\frac{3^{m+1}-1}{2}$ 时，由 (1) 可知 $1,3,\cdots,3^{m-1},3^m$ 就是一种砝码的组成方式. 下面我们证明 $1,3,\cdots,3^{m-1},3^m-1$ 也是一种方式.

若 $1\leqslant l\leqslant\frac{3^m-1}{2}$，由 (1) 可知

$l=\sum_{i=1}^{m}x_i3^{i-1},x_i\in\{-1,0,1\}$，则 $l=\sum_{i=1}^{m}x_i3^{i-1}+0\cdot(3^m-1)$；

若 $\frac{3^m-1}{2}<l\leqslant n<\frac{3^{m+1}-1}{2}$，则 $\frac{3^m-1}{2}<l+1\leqslant\frac{3^{m+1}-1}{2}$.

由(1)可知 $l+1=\sum_{i=1}^{m+1}x_i3^{i-1}$，其中 $x_i\in\{-1,0,1\}$，

易知 $x_{m+1}=1$.（否则 $l\leqslant\sum_{i=1}^{m}3^{i-1}-1=\frac{3^m-1}{2}-1$，矛盾）

则 $l=\sum_{i=1}^{m}x_i3^{i-1}+1\cdot(3^m-1)$.

所以，当 $n\neq\frac{3^m-1}{2}$ 时，$f(n)$ 块砝码的组成方式不唯一.

其次，下面我们证明：当 $n=\frac{3^m-1}{2}$ 时，$f(n)=m$ 块砝码的组成方式是唯一的，即

$a_i=3^{i-1}(1\leqslant i\leqslant m)$.

若对每个 $-\frac{3^m-1}{2}\leqslant l\leqslant\frac{3^m-1}{2}$，都有 $l=\sum_{i=1}^{m}x_ia_i,x_i\in\{-1,0,1\}$，即

$\left\{\sum_{i=1}^{m}x_ia_i \mid x_i\in\{-1,0,1\}\right\}\supseteq\left\{0,\pm1,\cdots,\pm\frac{3^m-1}{2}\right\}$.

注意左边集合中至多有 3^m 个元素，故必有

$\left\{\sum_{i=1}^{m}x_ia_i \mid x_i\in\{-1,0,1\}\right\}=\left\{0,\pm1,\cdots,\pm\frac{3^m-1}{2}\right\}$.

从而，对每个 l，$-\frac{3^m-1}{2}\leqslant l\leqslant\frac{3^m-1}{2}$，都可以唯一地表示为

$l=\sum\limits_{i=1}^{m}x_ia_i$，其中 $x_i\in\{-1,0,1\}$.

因而，$\sum\limits_{i=1}^{m}a_i=\frac{3^m-1}{2}$，则

$$\sum_{i=1}^{m}(x_i+1)a_i=\sum_{i=1}^{m}x_ia_i+\sum_{i=1}^{m}a_i=\sum_{i=1}^{m}x_ia_i+\frac{3^m-1}{2}.$$

令 $y_i=x_i+1$，则 $y_i\in\{0,1,2\}$.

由上可知，对每个 $0\leqslant l\leqslant 3^m-1$，都可以唯一地表示为

$l=\sum\limits_{i=1}^{m}y_ia_i$，其中 $y_i\in\{0,1,2\}$.

特别地，易知 $1\leqslant a_1<a_2<\cdots<a_m$.

下面用数学归纳法证明 $a_i=3^{i-1}(1\leqslant i\leqslant m)$.

当 $i=1$ 时，易知 $\sum\limits_{i=1}^{m}y_ia_i$ 中最小的正整数是 a_1，故 $a_1=1$.

假设当 $1\leqslant i\leqslant p$ 时，$a_i=3^{i-1}$.

由于 $\sum\limits_{i=1}^{p}y_ia_i=\sum\limits_{i=1}^{p}y_i3^{i-1}$，$y_i\in\{0,1,2\}$ 就是数的三进制表示，易知它们正好是 0，1，2，…，3^p-1，故 a_{p+1} 应是除上述表示外 $\left\{\sum\limits_{i=1}^{m}y_ia_i \mid y_i\in\{0,1,2\}\right\}$ 中最小的数，因此，$a_{p+1}=3^p$.

由数学归纳法可知，$a_i=3^{i-1}(1\leqslant i\leqslant m)$.

综上可知，当且仅当 $n=\frac{3^m-1}{2}$ 时，上述 $f(n)$ 块砝码的组成方式是唯一确定的.

【解题思维策略分析】

1. 注意发掘 p 进位制数的特殊性质

例 10 （1982 年英国数学奥林匹克题）17 的一个倍数写 2 进制数时恰好含有三个数字 1，证明它至少含有六个数字 0，而如果它恰好含有七个数字 0，那么它就是偶数.

解 $17=2^4+1$，写成二进制数为 $(10001)_2$，只含有两个数字 1. 考虑它的倍数 $17m$，如果写成二进制数而含有三个数字 1，那么 m 写成二进制数时必至少含有两个数字 1，于是可设

$17m=(2^4+1)(2^n+\cdots+1)\cdot 2^p$，

其中 n 是正整数，p 是正整数或零．上式展开后也可以整理成为 2 的不同次幂的和，这时项数就是相应的二进制数中所含数字 1 的个数．由于因数 2^p 不影响展开式的项数，我们只要考虑 $(2^4+1)(2^n+\cdots+1)=2^{4+n}+\cdots+2^4+2^n+\cdots+1$，按题设，此式可写成 2 的三个不同次幂（包括 $2^0=1$）的和．由此可见 n 不能小于 4，否则上式中至少有四项不能合并，违背题设．当 $n\geqslant 4$ 时，$2^{4+n}\geqslant 2^8$，上式相应的二进制数至少是九位数，如果其中恰有三个数字 1，就至少有六个数字 0．这样的 17 的倍数确定存在，例如 $17^2=(2^4+1)^2=2^8+2^5+1$．

如果二进制数恰含有三个数字 1 和七个数字 0，那么它是十位数；设为奇数，则可表示为 2^9+2^n+1，其中 n 是小于 9 的正整数．但是不难验证，$n=1$，2，3，4，5，6，7，8 时，2^9+2^n+1 都不是 17 的倍数．因此，这样的 17 的倍数只能是偶数，例如 $2(2^8+2^5+1)=2^9+2^6+2$．

例 11 （IMO－35 试题）对于任何正整数 k，$f(k)$ 表示集合 $\{k+1,k+2,\cdots,2k\}$ 内在二进制表示下恰有 3 个 1 的所有元素的个数．

（1）求证：对于每个正整数 m，至少存在一个正整数 k，使得 $f(k)=m$．

（2）确定所有正整数 m，对每一个 m，恰存在一个 k，满足 $f(k)=m$．

证明 用 S 表示正整数集合内在二进制表示下恰有 3 个 1 的所有元素组成的集合．首先证明

$$f(k+1)=\begin{cases}f(k),当 2k+1\notin S,\\ f(k)+1,当 2k+1\in S.\end{cases} \qquad ①$$

由于 $f(k+1)$ 是集合 $\{k+2,k+3,\cdots,2k+1,2k+2\}$ 内在二进制表示下恰有 3 个 1 的所有元素组成的集合，$f(k)$ 是集合 $\{k+1,k+2,\cdots,2k\}$ 内在二进制表示下恰有 3 个 1 的所有元素组成的集合．在二进制表示下，在 $k+1$ 的个位数后面添加一个零，恰为 $2(k+1)$ 在二进制表示下的数字．于是，$k+1$ 与 $2(k+1)$ 同属于 S，或者同时不属于 S，因此有①．

（1）显然 $f(1)=0$，$f(2)=0$．当 $k=2^s$，s 是大于等于 2 的正整数时，$f(2^s)$ 表示集合 $\{2^s+1,2^s+2,\cdots,2^{s+1}\}$ 内在二进制表示下恰有 3 个 1 的所有元素的个数．

在二进制表示下，

$$2^s+1=1\underbrace{0\cdots0}_{s-1}1,\quad 2^{s+1}=1\underbrace{0\cdots0}_{s+1}.$$

考虑所有形如 1 * * … * 的 $s+1$ 位数，取 2 个 1 放入这 s 个 * 中的任两个 * 位置，其余 * 位置全部放入 0，就得到集合 $\{2^s+1,\ 2^s+2,\ \cdots,\ 2^{s+1}\}$ 内在二进制表示下恰有 3 个 1 的一个元素，于是，

$$f(2^s)=C_s^2=\frac{1}{2}s(s-1).$$

当 s 增大时，$\frac{1}{2}s(s-1)$ 显然无上界. 从①可知 $f(k)$ 无上界. 又从 $f(1)=0$，$f(k)$ 无上界及①可知，当 k 取遍所有正整数时，$f(k)$ 取遍所有非负整数. 于是，对于每个正整数 m，至少存在一个正整数 k，满足 $f(k)=m$.

(2) 由于对每一个 m，恰存在一个 k，满足 $f(k)=m$，则由①可知，

$f(k+1)=f(k)+1=m+1$ 及 $f(k-1)=f(k)-1=m-1$.

这表明 $2k+1\in S$，$2(k-1)+1\in S$.

设在二进制下，$k=2^s+k_1 2^{s-1}+k_2 2^{s-2}+\cdots+k_{s-1}2+k_s$，

这里 k_1，k_2，…，$k_s\in\{0,1\}$，s 是正整数.

$2k-1=2^{s+1}+k_1 2^s+k_2 2^{s-1}+\cdots+k_{s-1}2^2+k_s 2-1$，

$2k+1=2^{s+1}+k_1 2^s+k_2 2^{s-1}+\cdots+k_s 2+1$.

由于在二进制下，$2k+1$ 恰有 3 个 1，则 k_1，k_2，…，k_s 中只有一个为 1，其余皆为 0. 于是，$2k+1=2^{s+1}+2^t+1$，这里 t 是小于等于 s 的正整数. 那么，

$$k=2^s+2^{t-1}，\qquad ②$$

$$2k-1=2^{s+1}+2^t-1=2^{s+1}+2^{t-1}+\cdots+2+1. \qquad ③$$

由于在二进制下，$2k-1$ 也恰有 3 个 1，则 $t=2$. 从而，$s\geqslant 2$，由②有

$$k=2^s+2，k+1=2^s+2+1，2k=2^{s+1}+2^2. \qquad ④$$

在二进制下，$k+1$ 为 $10\cdots011$(有 $s-2$ 个 0)，$2k$ 为 $10\cdots0100$(一共有 s 个 0). 在 $k+1$ 与 $2k$ 之间的正整数为 $1**\cdots*$(有 s 个 $*$，但排除 $10\cdots000$，$10\cdots001$，$10\cdots010$ 三个数)，及 $s+2$ 位数 $10\cdots01$，$10\cdots010$，$10\cdots011$，因此，

$$f(2^s+2)=C_s^2+1=\frac{1}{2}s(s-1)+1. \qquad ⑤$$

从而，$f(k)=m$ 恰有唯一解时，必有 $m=\frac{1}{2}s(s-1)+1$，这里 $s\geqslant 2$.

当 $m=\frac{1}{2}s(s-1)+1$ 时，取 $k=2^s+2$，从上述证明得

$$f(2^s+2)=\frac{1}{2}s(s-1)+1.$$

由于 $2(2^s+2)-1=2^{s+1}+2+1$，$2(2^s+2)+1=2^{s+1}+2^2+1$

都恰有 3 个 1，则由①，有

$$f(2^s+2-1)=f(2^s+2)-1，f(2^s+2+1)=f(2^s+2)+1.$$

从而，$f(k)=\frac{1}{2}s(s-1)+1$ 的确有唯一解 $k=2^s+2$，这里正整数 $s\geqslant 2$.

2. 注意发掘题设条件中隐含有 p 进位制数背景

例 12 (2008 年中国女子数学奥林匹克题) 对于正整数 n，令 $f_n=[2^n\sqrt{2008}]+$

$[2^n\sqrt{2009}]$. 求证：数列 $f_1, f_2, \cdots$ 中有有穷多个奇数和无穷多个偶数.（$[x]$表示不超过 x 的最大整数）

证明 由于题设中含有“2^n”，不妨设将 $\sqrt{2008}$ 和 $\sqrt{2009}$ 化为二进制后的无限小数为 a_1 和 a_2.

我们知道，这两个小数都是不循环的，而 f_n 是奇还是偶，取决于 a_1 和 a_2 小数点后的第几位是否相同. 如果数列 f_1，f_2，…中有有限个奇数，那么在某个 n 以后，所有的 f_k 都是偶数，这说明在小数点后 n 位开始，a_1 和 a_2 的每一位都相同. 这说明 a_2-a_1 在二进制下是有限小数，即是一个有理数，但这显然是不可能的. 如果数列 f_1，f_2，…中只有有限个偶数，在某个 n 以后，所有的 f_k 都是奇数，这说明在小数点后 n 位开始，a_1 和 a_2 的每一位都不同. 这说明 a_2+a_1 在二进制下是有限小数，即是一个有理数，这显然也是不可能的. 至此，便证明了原命题成立.

例 13 （*1989 年爱尔兰数学奥林匹克题*）函数 f 定义在自然数集上，且满足下列条件：

(1) $f(1)=1$；

(2) $f(2n)=f(n), f(2n+1)=f(2n)+1(n\geqslant 1)$.

当 $1\leqslant n\leqslant 1989$ 时，试求出 $f(n)$ 的最大数 u，并且求出有多少个 $n(1\leqslant n\leqslant 1989)$，使 $f(n)=n$.

解 我们来证明：若 a 是用二进制表示的数，则 $f(a)$ 是 a 的各位数字之和. 事实上，当 a 是个位数时，$f(1)=1$，命题成立；假设 a 是 n 位数时，命题成立，即

当 $a=a_1 2^{n-1}+a_1 2^{n-2}+\cdots+a_{n-1}$ 时，$f(a)=a_0+a_1+\cdots+a_{n-1}$.

二进制的 $n+1$ 位数有两种情况：

(i) $2a=a_0 2^n+a_1 2^{n-1}+\cdots+a_{n-1}\cdot 2$，它的各位数字之和为 $a_0+a_1+\cdots+a_{n-1}=f(a)$，又 $f(2a)=f(a)$，即 $f(2\cdot a)$的各位数字之和是 $2a$ 的各位数字之和.

(ii) $2a+1=a_0 2^n+a_1 2^{n-1}+\cdots+a_{n-1}\cdot 2+1$，它的各位数字之和是

$a_0+a_1+\cdots+a_{n-1}+1=f(a)+1$.

又 $f(2a+1)=f(2a)+1=f(a)+1$，即 $f(2a+1)$也是 $2a+1$ 的各位数字之和.

这样我们用数学归纳法证明了当 a 是用二进制表示的数时，$f(a)$是 a 的各位数字之和.

因为 $2^{10}+2^9+\cdots+2+1=2^{11}-1=2047>1989$，又

$1989=2^{10}+2^9+2^8+2^7+2^6+2^2+1=(11111000101)_2$，

所以 $M_{max}=10$.

不超过十进制 1989 的二进制为一个十位数，$(1111111111)_2=1023$ 和四个十一位数 $(10111111111)_2=1535$，$(11011111111)_2=1791$，$(11101111111)_2=1919$，$(11110111111)_2=1983$.

所以 $M_{max}=10$，当 $1\leqslant n\leqslant 1989$ 时，有 5 个 n 使 $f(n)=10$.

例 14 （IMO－29 试题）设 N 为正整数集，在 N 上定义函数 f 如下：

(i) $f(1)=1, f(3)=3$;

(ii) 对 $n\in\mathbf{N}$，有 $f(2n)=f(n), f(4n+1)=2f(2n+1)-f(n), f(4n+3)=3f(2n+1)-2f(n)$.

试求所有的 n，使 $n\leqslant 1988$ 且 $f(n)=n$.

解 由条件 (i) 和 (ii)，我们可经计算得下表：

n	1	2	3	4	5	6	7	8	9
$f(n)$	1	1	3	1	5	3	7	1	9

n	10	11	12	13	14	15	16	17	
$f(n)$	5	13	3	11	7	15	1	17	

把上表中的数改成二进制表示，我们又得

n	1	10	11	100	101	110	111	1000	1001
$f(n)$	1	1	11	1	101	11	111	1	1001

n	1010	1011	1100	1101	1110	1111	10000	10001	
$f(n)$	101	1101	11	1011	111	1111	1	10001	

于是，我们猜想：$f(n)$ 等于表示 n 的二进制数全部反序而得到的二进制数.

下面，我们先证明这个猜想是正确的.

事实上，当 $n=1$，3 时，上述猜想成立.

假设 $n<k$ 时上述猜想成立．我们来证明 $n=k$ 时上述猜想也成立.

事实上，如果 k 是偶数，那么可设 k 的二进制数为 $(a_la_{l-1}\cdots a_10)_2$，$\frac{k}{2}$ 的二进制数为 $(a_la_{l-1}\cdots a_1)_2$，此时根据已知条件和归纳假设可得 $f(k)=f\left(\frac{k}{2}\right)=(a_1\cdots a_{l-1}a_l)_2$，故 k 为偶数时，猜想成立.

如果 $k=4m+1(m\in\mathbf{N})$，那么可设 k 的二进制数为

$k=4m+1=(a_la_{l-1}\cdots a_201)_2$，

于是 $m=(a_la_{l-1}\cdots a_2)_2$，$2m+1=(a_la_{l-1}\cdots a_21)_2$，

此时，根据已知条件和归纳假设可得

$$f(4m+1)=2f(2m+1)-f(m)$$
$$=(1a_2\cdots a_{l-1}a_l0)_2-(a_2\cdots a_{l-1}a_l)_2=2^l+2f(m)-f(m)$$
$$=2^l+f(m)=(10a_2\cdots a_{l-1}a_l)_2.$$

这就是说，$k=4m+1$ 时猜想也成立.

同理可证，$k=4m+3$ 时猜想也成立.

根据数学归纳原理，猜想得到证明.

$n=(a_1a_2\cdots a_l)_2=(a_la_{l-1}\cdots a_1)_2$，即 $a_i=a_{l+1-i}$，$(i=1,2,\cdots,[\frac{l}{2}])$.

当 n 的二进制位数为偶数 $2s$ 时，满足上述条件的 n 是 2^{s-1} 个；当 n 的二进制位数为奇数 $2s+1$ 时，满足上述条件的 n 有 2^s 个.

注意到 $1988=(11111000100)_2$，而比这个数大的满足 $f(n)=n$ 的 11 位二进制数只有两个：$(11111111111)_2$ 和 $(11111011111)_2$，因此所求的数的个数为

$$(1+1+2+2+4+4+8+8+16+16+32)-2=92.$$

例 15 （IMO－37 预选题）设序列 $a(n)$，$n=1,2,3,\cdots$ 定义如下：

$a(1)=0$，并且当 $n>1$ 时，$a(n)=a([\frac{n}{2}])+(-1)^{\frac{n(n+1)}{2}}$.

(1) 求出 $a(n)$ 在 $n<1996$ 范围内的最大值和最小值，并给出取得这些极值的全部的 n 的值.

(2) 在 $n<1996$ 范围内，值为 0 的 $a(n)$ 有多少项?

解 由 $n>1$ 时，$a(n)=a([\frac{n}{2}])+(-1)^{\frac{n(n+1)}{2}}$，可得

$n\geqslant1$ 时，$a(2n)=a(n)+(-1)^{n(2n+1)}=a(n)+(-1)^n$.

$a(2n+1)=a(n)+(-1)^{(2n+1)(n+1)}=a(n)+(-1)^{n+1}$.

设 $n\geqslant2$ 时，n 在二进制表示下为 $(a_1a_2\cdots a_l)_2$，其中 $a_i=0$ 或 1，$i=1,2,\cdots,l$. 考虑 $l-1$ 个数码对

$(a_1,a_2),(a_2,a_3),\cdots,(a_{l-1},a_l)$.

设其中满足 $a_k=a_{k+1}$ 的有 $f(n)$ 个，满足 $a_k\neq a_{k+1}$ 的有 $g(n)$ 个，$k=1,2,\cdots,l-1$. 显然，$f(n)+g(n)=l-1$.

下面用归纳法证明：$n\geqslant2$ 时，有 $a(n)=f(n)-g(n)$. ①

事实上，$a(2)=a(1)+(-1)^1=-1$，$a(3)=a(1)+(-1)^2=1$.

又 $f(2)=0$，$g(2)=1$，$f(3)=1$，$g(3)=0$，因此当 $n=2,3$ 时，①式成立.

假设对于某个 $k\geqslant3$，当 $2\leqslant n\leqslant k$ 时，①式成立. 考虑 $n=k+1$ 时的情况.

设 $k+1=(a_1a_2\cdots a_l)_2$，$l\geqslant3$，则

$a(k+1)=a((a_1a_2\cdots a_l)_2)=a((a_1a_2\cdots a_{l-1})_2)+(-1)^{(a_1a_2\cdots a_{l-1})_2+a_l}$

$=f((a_1a_2\cdots a_{l-1})_2)-g((a_1a_2\cdots a_{l-1})_2)+(-1)^{a_{l-1}+a_l}$.

若 $a_{l-1}=a_l$，则 $f(k+1)=f((a_1a_2\cdots a_{l-1})_2)$，

$g(k+1)=g((a_1a_2\cdots a_{l-1})_2)+1$.

于是 $a(k+1)=f((a_1a_2\cdots a_{l-1})_2)-g((a_1a_2\cdots a_{l-1})_2)-1$

$=f(k+1)-g(k+1)$.

因此 $n=k+1$ 时，①式也成立.

(1) 因为 $(1995)_{10}=(11111001011)_2$，而由①式知当且仅当 $n=(1111111111)_2=1023$ 时，$a(n)$ 取最大值 9；$n=(10101010101)_2=1365$ 时，$a(n)$ 取最小值 -10.

(2) 设 $n=(a_1a_2\cdots a_l)_2$，$n\geqslant2$，则当且仅当 $f(n)=g(n)$ 时，$a(n)=0$，此时

$l-1=f(n)+g(n)=2f(n)$，为偶数，从而 l 是奇数.

当 $2\leqslant n\leqslant1995$ 时，l 只能取 3，5，7，9，11.

对于固定的 $l\in\{3,5,7,9,11\}$，当 $2^{l-1}\leqslant n\leqslant2^l-1$ 时，n 在二进制表示下为 $(a_1a_2\cdots a_l)_2$，且 $a_1=1$，故当且仅当恰有 $\frac{l-1}{2}$ 个数码对 (a_k,a_{k+1}) 满足 $a_k=a_{k+1}$ 时 $a(n)=0$. 因此，$2^{l-1}\leqslant n\leqslant2^l-1$ 时，值为 0 的 $a(n)$ 共有 $C_{l-1}^{\frac{l-1}{2}}$ 项，于是，当 $2\leqslant n\leqslant2^{11}-1$ 时，值为 0 的 $a(n)$ 共有

$C_2^1+C_4^2+C_6^3+C_8^4+C_{10}^5=350$(项).

当 $1996\leqslant n\leqslant2^{11}-1$ 时，易知只有取

$(11111101010)_2$，$(11111011010)_2$，$(11111010110)_2$，$(11111010010)_2$，$(11111010100)_2$ 这 5 个值，$a(n)=0$.

故当 $2\leqslant n\leqslant1995$ 时，值为 0 的 $a(n)$ 项有 345 项，又 $a(1)=0$，因此，当 $n<1996$ 时，值为 0 的 $a(n)$ 共 346 项.

【模拟实战】

习题 A

1. (1988 年上海市数学竞赛题) 求满足 $\overline{abc}=(a+b+c)^3$ 的所有三位数 $\overline{abc}$.
2. (第 9 届加拿大数学竞赛题) N 是整数，它的 b 进制表示是 777. 求最小的正整数 b，使得 N 为十进制整数的四次方.
3. (1991 年日本数学奥林匹克题) n 为非负整数，由 $f(0)=0$，$f(1)=1$，$f(n)=f\left(\left[\frac{n}{2}\right]\right)+n-2\left[\frac{n}{2}\right]$ 确定 $f(n)$. 求在 $0\leqslant n\leqslant1991$ 时，$f(n)$ 的最大值. (这里 $[x]$ 表示不超过 x 的最大整数)

4.（基辅市数学竞赛题）（1）在几进位制中，16324 是 125 的平方？

（2）在几进位制中，$4 \cdot 13=100$？

5. 设 1993 可以在 b 进位制中写成三位数 $\overline{xyz}$，且 $x+y+z=1993$. 试确定出所有可能的 x，y，z 和 b.

6.（IMO－5 试题）（1）求所有的正整数 n，使得 2^n-1 能被 7 整除；

（2）证明：对于任何正整数 n，2^n+1 不能被 7 整除.

7.（IMO－10 试题）设$[x]$表示不超过 x 的最大整数，试求 $\sum\limits_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]$ 的值，其中 n 是任意自然数.

8. 1500 只产品分装 15 箱出厂，在包装密封完毕后，发现还有一只产品未装入箱内. 因包装密封要求很高，不允许逐箱打开检查，有人提出用磅秤称各箱的重量来检查（因为少装一只产品的一箱较轻），按通常的方法每箱称一次要称 14 次才能把少装的一箱检查出来，问有没有办法减少称的次数而仍能把少装的一箱检查出来.

9.（第 24 届全美数学竞赛题）现有 1990 堆石头，块数分别为 1，2，…，1990，进行如下操作，每次可选择任意多堆，从其中每堆拿走同样多石块，问要把所有石块都拿走，最少要操作多少次？

10.（基辅市数学竞赛题）有一个写成七进制的三位数，如果把各位数码按相反顺序写出，并把它看成九进制的三位数，且这两数相等，求这个数.

11.（1991 年南昌市数学竞赛题）现有一大缸水和 5 个量杯，量杯的容积依次为 1，5，25，125，625（毫升）. 试证明对于不超过 1562 的整数 a，只要用这 5 个量杯，每个至多用 2 次，就能把 a 毫升的水注入空水桶中.（说明：从大缸量一杯水倒入水桶，或从水桶量一杯水倒入大缸，均算用量杯一次.）

12. 证明：当 $n\geqslant2$ 时，Fermat 数 $F_n=2^{2^n}+1$ 的末位数都是 7.

13.（第 17 届加拿大数学奥林匹克题）求证：2^{n-1}能整除 $n!$ 的一个必要充分条件是 $n=2^{n-1}$，这里 k 为某一自然数.

14.（IMO－30 预选题）设 m 为正奇数，求使 2^{1989} 整除 m^n-1 的最小的自然数 n.

15.（IMO－29 预选题）对每个正整数 k，n，令 $S_k(n)$表示 n 在 k 进制中的数字和. 证明对小于 20000 的素数 p，$S_{31}(p)$至多有两个值为合数.

16.（IMO－12 试题）设 a，b，n 都是自然数，并且 $a>1$，$b>1$，$n>1$，又 A_{n-1} 和 A_n 是 a 进制数，B_{n-1} 和 B_n 是 b 进制数，并且 A_{n-1}，A_n，B_{n-1} 和 B_n 可以表示为如下形式：

$A_{n-1}=\overline{x_{n-1}x_{n-2}\cdots x_0}$，$A_n=\overline{x_nx_{n-1}\cdots x_0}$（$a$ 进制写出）.

$B_{n-1}=\overline{x_{n-1}x_{n-2}\cdots x_0}$，$B_n=\overline{x_nx_{n-1}\cdots x_0}$（$b$ 进制写出），此处 $x_n\neq0$，$x_{n-1}\neq0$.

试证：当 $a>b$ 时，$\frac{A_{n-1}}{A_n}<\frac{B_{n-1}}{B_n}$.

17. （IMO－24 试题）能否选择 1983 个不同的正整数，使它们都不大于 10^5 且其中任何三数都不是等差数列中的连续项？证明你的结论.
18. （IMO－28 预选题）找出 8 个正整数 n_1，n_2，…，n_8，使它们有下列性质：对于每个整数 k，$-1985\leqslant k\leqslant 1985$，有 8 个整数 a_1，a_2，…，a_8，其中每个 a_i 都属于集合 $\{-1,0,1\}$，使得 $k=\sum_{i=1}^{8}a_in_i$.
19. （1985 年英国数学奥林匹克题）一个正整数称为"坏数"，如果它的二进制表示中数码 1 的个数是偶数，例如 $18=(10010)_2$ 是"坏数". 在正整数集合中，求前 1985 个"坏数"之和.

习题 B

1. （第 48 届斯洛文尼亚数学奥林匹克题）求所有满足以下条件的三位数：该数等于它的各位数字之和的 30 倍.
2. （2005 年日本数学奥林匹克题）对自然数 n，用 $S(n)$表示其各位数字之和，例如 $S(611)=6+1+1=8$. 设 a,b,c 均为三位数，使得 $a+b+c=2005$，而 M 为 $S(a)+S(b)+S(c)$的最大值. 问有多少组(a,b,c)满足 $S(a)+S(b)+S(c)=M$?
3. （2003 年泰国数学奥林匹克题）在有理数集中定义：$f(0)=0$，$f(1)=1$，

$$f(x)=\begin{cases}\frac{f(2x)}{4},0<x<\frac{1}{2};\\ \frac{3}{4}+\frac{f(2x-1)}{4},\frac{1}{2}\leqslant x<1.\end{cases}$$

若用二进制表示 x，如 $x=(0.b_1b_2b_3\cdots)_2$，求二进制表示的 $f(x)$.
4. （CMO－24 试题）给定整数 n（$n\geqslant 3$）. 证明：存在 n 个互不相同的正整数组成的集合 S，使得对 S 的任意两个不同的非空子集 A，B，数

$$\frac{\sum\limits_{x\in A}x}{|A|}\text{ 与 }\frac{\sum\limits_{x\in B}x}{|B|}$$

是互素的合数（这里 $\sum\limits_{x\in X}x$ 与 $|X|$ 分别表示有限数集 X 的所有元素之和及元素个数）.
5. （第 12 届土耳其数学奥林匹克题）已知集合 $K(n,0)=\varnothing$. 对于任意非负整数 m，n，定义 $K(n,m+1)=\{k|1\leqslant k\leqslant n,K(k,m)\cap K(n-k,m)=\varnothing\}$，求集合 $K(2004,$

2004)中元素的个数.

6. (2003 年白俄罗斯数学奥林匹克题) (1) 如果一个正整数能表示为一些正整数(这些正整数均为 2 的非负整数次幂，且可以相同) 的算术平均，则称这个正整数为“好数”. 证明：所有正整数均为“好数”.

(2) 如果一个正整数不能表示为一些两两不同的正整数 (这些正整数均为 2 的非负整数次幂) 的算术平均，则称这个正整数为“坏数”. 证明：存在无穷多个“坏数”.

7. (2006 年捷克-波兰-斯洛伐克数学奥林匹克题) 证明：对于每一个整数 k ($k\geqslant1$)，存在一个满足下列性质的正整数 n：

用十进制表示 2^n，可以恰好含有 k 个连续 0 的单位，即 $2^n=\cdots a\underbrace{00\cdots0}_{k个}b\cdots$，

其中，a、b 是非零数字.

8. (2002—2003 年度匈牙利数学奥林匹克决赛题) 设 t 是一个固定的正整数，$f_t(n)$ 表示满足 C_k^t 是奇数的数目，其中 $1\leqslant k\leqslant n$，k 为整数. 若 $1\leqslant k<A$，则规定 $C_k^t=0$. 证明：如果 n 是一个足够大的 2 的整数次幂，则 $\dfrac{f_t(n)}{n}=\dfrac{1}{2^r}$，其中 r 是一个依赖于 t，但不依赖于 n 的整数.

9. (2007 年保加利亚国家数学竞赛题) 已知整数 k ($k>5$)，用 k 进制表示给定的正整数，将这个 k 进制的数的各位数码之和与 $(k-1)^2$ 的积写在给定的正整数的后面，对所得到的新的数继续这种运算得到一个数列. 证明：从某个数开始，其后面的数全部相等.

10. (第 11 届土耳其数学奥林匹克题) 求方程 $x^m=2^{2n+1}+2^n+1$ 的三元正整数解 (x, m, n).

11. (2007 年波罗的海地区数学竞赛题) 设 r, k 是正整数，且 r 的所有素因数比 50 大. 一个正整数在十进制表示下至少有 k 位数 (首位数不是零)，如果其十进制表示下的每个连续的 k 个数码组成的整数 (可能首位数是零) 都是 r 的倍数，则称为“好数”. 证明：如果存在无穷多个好数，则 10^k-1 是好数.

12. (第 24 届伊朗数学奥林匹克题) 对 $A\subseteq\mathbf{Z}$ 和 a, $b\in\mathbf{Z}$，记 $aA+b$ 表示集合$\{ax+b \mid x\in A\}$. 若 $a\neq0$，称集合 $aA+b$ 与 A“相似”. “康托集”C 是由三进制表示中不含 1 的非负整数构成的集合.

易知，$C=(3C)\cup(3C+2)$.

另一个例子是

$C=(9C)\cup(9C+6)\cup(3C+2)$.

集合 C 的表示是指将 C 划分为有限个(多于 1 个)与 C 相似的集合，即

$$C=\bigcup_{i=1}^{n}C_i,$$

其中，$C_i=a_iC+b_i$ 是与 C 相似的集合.

当且仅当某些 C_i 的并集不与 C 相等或相似时，称 C 的一个表示是“本原的”.

考虑康托集的一个本原的表示. 求证：

(1) $a_i>1$；

(2) 所有 a_i 都是 3 的方幂；

(3) $a_i>b_i$；

(4) C 的唯一的本原的表示是 $C=(3C)\cup(3C+2)$.

13. (2005 年全国高中数学联赛题) 记集合 $T=\{0,1,2,3,4,5,6\}$，$M=\left\{\frac{a_1}{7}+\frac{a_2}{7^2}+\frac{a_3}{7^3}+\frac{a_4}{7^4}\middle|a_i\in T,i=1,2,3,4\right\}$，将 M 中的元素按从大到小的顺序排列，则第 2005 个数是 (　　).

A. $\frac{5}{7}+\frac{5}{7^2}+\frac{6}{7^3}+\frac{3}{7^4}$　　B. $\frac{5}{7}+\frac{5}{7^2}+\frac{6}{7^3}+\frac{2}{7^4}$

C. $\frac{1}{7}+\frac{1}{7^2}+\frac{0}{7^3}+\frac{4}{7^4}$　　D. $\frac{1}{7}+\frac{1}{7^2}+\frac{0}{7^3}+\frac{3}{7^4}$

14. (2004 年国家队数学培训题) 证明存在正整数 m，使得 2004^m 的十进制表示的开始的数字为 20 042 005 200 620 072 008.

15. (2004 年国家队选拔赛题) 已知 p_1，p_2，…，p_{25} 为给定的不超过 2004 的 25 个互不相同的素数，求最大的整数 T，使得任何不大于 T 的正整数总可以表示成 $(p_1p_2\cdots p_{25})^{2004}$ 的互不相同的正约数之和. [如 1，p_1，$1+p_1^2+p_1p_2+p_3$ 等均是 $(p_1p_2\cdots p_{25})^{2004}$ 的互不相同的正约数之和.]

16. (2008 年国家队数学培训题) 记 $A=\{x\mid x\in\mathbf{N}^*$，在十进制表示下 x 的每一个数码都不是零，且 $S(x)\mid x\}$，这里 $S(x)$ 表示 x 的各数码之和.
求证：对任意正整数 k，A 中都有一个恰好是 k 位的正整数.

17. (2005 年国家队数学培训题) 互素正整数 p_n，q_n 满足 $\frac{p_n}{q_n}=1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$，试找出所有的正整数 n，使得 $3\mid p_n$.

第十七章　不定方程

【基础知识】

不定方程是指未知数的个数多于方程的个数，且它们的解受到某种限制的方程. 通常研究的是不定方程的正整数解、整数解、有理数解等. 不定方程也称为丢番图方程，是数论的重要分支学科，是历史上最活跃的数学领域之一. 不定方程的内容极其丰富，与代数数论、代数几何、集合数学等有密切的联系. 不定方程的重要性在数学竞赛中也得到了充分的体现，每年世界各地的数学竞赛中，不定方程的问题都占有一席之地；它也是培养和考查学生数学思维能力的好材料，数学竞赛中的不定方程问题，不仅要求选手对初等数论的一般理论、方法要有一定的了解，而且更需要讲究思想、方法与技巧，创造性地解决相关问题.

1. 不定方程问题的常见类型

(1) 求不定方程的解；

(2) 判定不定方程是否有解；

(3) 判定不定方程的解的数量（有限还是无限).

2. 不定方程问题的常用解法

(1) 代数恒等变形，如因式分解、配方、换元等方法；

(2) 不等式估计法：利用不等式等方法，确定出方程中某些变量的范围，进而求解；

(3) 同余法：对等式两边取特殊的模（如奇偶分析)，缩小变量的范围或性质，得出不定方程的整数解或判定其无解；

(4) 构造法：构造出符合要求的特解，或构造一个求解的递推式，证明方程有无穷多解；

(5) 无穷递降法.

不定方程理论中，有如下几个关于特殊方程的求解定理.

3. 二元一次不定方程

定义 1　形如 $ax+by=c$（a，b，$c\in \mathbf{Z}$，a、b 不同时为零）的方程称为二元一次不定方程.

定理 1 不定方程 $ax+by=c$ 有整数解的充要条件是 $(a,b)\mid c$.

证明 必要性是显然的，下证充分性.

设 $(a,b)=d$, $a=a_1d$, $b=b_1d$, $c=c_1d$，于是原方程可化为

$a_1x+b_1y=c_1$, $(a_1,b_1)=1$.

因 $(a_1,b_1)=1$，由裴蜀定理知，存在整数 x_0', y_0'，使得 $a_1x_0'+b_1y_0'=1$，

所以 $a_1(c_1x_0')+b_1(c_1y_0')=c_1$，

从而，$x_0=c_1x_0'$, $y_0=c_1y_0'$ 就是原方程的整数解.

定理 2 设 x_0，y_0 是方程 $ax+by=c$ 的一组整数解，则此方程的一切整数解可表示为

$$\begin{cases} x=x_0+\dfrac{b}{(a,b)}t, \\ y=y_0-\dfrac{a}{(a,b)}t, \end{cases} t\in\mathbf{Z}. \qquad ①$$

证明 因 x_0, y_0 是一组解，所以 $ax_0+by_0=c$，因此

$$a\left(x_0+\frac{b}{(a,b)}t\right)+b\left(y_0-\frac{a}{(a,b)}t\right)=ax_0+by_0=c,$$

这表明①是方程的解.

设 x', y' 是方程的任一整数解，则有 $ax'+by'=c$.

把它与原方程相减，得 $a(x'-x_0)=-b(y'-y_0)$，

所以 $\dfrac{a}{(a,b)}\mid y'-y_0$.

令 $y'-y_0=-\dfrac{a}{(a,b)}t$，得 $x'-x_0=\dfrac{b}{(a,b)}t$，所以

$x'=x_0+\dfrac{b}{(a,b)}t$，$y'=y_0-\dfrac{a}{(a,b)}t$.

因此，x', y' 可表示为①的形式，从而命题得证.

4. 勾股数方程

定义 2 形如 $x^2+y^2=z^2$ 的方程叫做勾股数方程，这里 x，y，z 为正整数，并称满足条件 $(x,y)=1$ 的解为方程的基本解.

定理 3 勾股数方程 $x^2+y^2=z^2$ 满足条件 $2\mid y$ 的一切基本解可表示为

$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2, \qquad (*)$$

其中 $a>b>0$, $(a,b)=1$，且 a, b 为一奇一偶.

证明 定理包含两部分内容：其一，当 a，b 满足条件时，由（*）给出的 (x, y, z) 是勾股数方程的解；其二，对于勾股数方程的任一解 (x, y, z)，必可找到满足要求的 a，b，使 x，y，z 可表示成（*）的形式. 前者是明显的，下证后者.

由（*）知 x，y，$z>0$，且 $2\mid y$. 若 $(x,z)=d$，则 $d\mid x$, $d\mid z$，即

$d\mid(a^2-b^2)$, $d\mid(a^2+b^2)$.

从而 $d|2a^2$，$d|2b^2$，故 $d|2(a^2,b^2)$. 由 $(a,b)=1$ 知 $(a^2,b^2)=1$，从而 $d|2$，但 a，b 一奇一偶，故 x 为奇数，所以 $d=1$.

另外，设 (x,y,z) 是勾股数方程的任意一组满足 $2|y$ 的基本解. 因 y 为偶数，故 x，z 为奇数，且 $(x,z)=1$，此时 $\frac{z-x}{2}$，$\frac{z+x}{2}$ 均为整数，且

$$\left(\frac{z-x}{2},\frac{z+x}{2}\right)=\left(\frac{z-x}{2}+\frac{z+x}{2},2\cdot\frac{z+x}{2}\right)=(z,z+x)=(z,x)=1.$$

又 $\frac{z-x}{2}\cdot\frac{z+x}{2}=\left(\frac{y}{2}\right)^2$，所以 $\frac{z-x}{2}$，$\frac{z+x}{2}$ 都是完全平方数，即存在整数 $a>b>0$，使得

$$\frac{z+x}{2}=a^2,\ \frac{z-x}{2}=b^2,\ \frac{y}{2}=ab.$$

所以 $x=a^2-b^2$，$y=2ab$，$z=a^2+b^2$.

又由于 z 是奇数，故 a，b 一奇一偶，且

$$(a^2,b^2)=\left(\frac{z+x}{2},\frac{z-x}{2}\right)=1,\text{故}(a,b)=1.$$

由定理 3 可得勾股数方程的所有解.

推论 勾股数方程 $x^2+y^2=z^2$ 的全部正整数解（x，y 的顺序不加区别）可表示为 $x=(a^2-b^2)d$，$y=2abd$，$z=(a^2+b^2)d$，其中 $a>b>0$ 是互素的奇偶性不同的一对正整数，d 是一个正整数.

5. 佩尔（Pell）方程

定义 3 通常 Pell 方程是指下面四个不定方程：

$x^2-dy^2=\pm1,\pm4(x,y\in\mathbf{Z},d\in\mathbf{N}^*$ 且不是平方数).

如果上述 Pell 方程有正整数解 (x,y)，则称使 $x+\sqrt{d}y$ 最小的正整数解 (x_1,y_1) 为它的最小解.

定理 4 Pell 方程 $x^2-dy^2=1$($d\in\mathbf{N}^*$ 且不是平方数)必有正整数解 (x,y)，且若设它的最小解为 (x_1,y_1)，则它的全部解可以表示成

$$\begin{cases}x_n=\frac{1}{2}[(x_1+\sqrt{d}y_1)^n+(x_1-\sqrt{d}y_1)^n],\\ y_n=\frac{1}{2\sqrt{d}}[(x_1+\sqrt{d}y_1)^n-(x_1-\sqrt{d}y_1)^n],\end{cases}(n\in\mathbf{N}^*).$$

上面的公式也可写成如下几种形式：

(1) $x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n$.

(2) $\begin{cases}x_{n+1}=x_1x_n+dy_1y_n,\\ y_{n+1}=x_1y_n+y_1x_n.\end{cases}$

(3) $\begin{cases} x_{n+1}=2x_1x_n-x_{n-1}, \\ y_{n+1}=2x_1y_n-y_{n-1}. \end{cases}$

定理 5 佩尔方程 $x^2-dy^2=-1$（$d\in\mathbf{N}^*$ 且不是平方数）要么无正整数解，要么有无穷多组正整数解 (x, y).

在后一种情况下，设它的最小解为 (x_1, y_1)，则它的全部解可以表示为

$$\begin{cases} x_n=\dfrac{1}{2}\left[(x_1+\sqrt{d}y_1)^{2n-1}+(x_1-\sqrt{d}y_1)^{2n-1}\right], \\ y_n=\dfrac{1}{2\sqrt{d}}\left[(x_1+\sqrt{d}y_1)^{2n-1}-(x_1-\sqrt{d}y_1)^{2n-1}\right], \end{cases} \quad (n\in\mathbf{N}^*).$$

6. 费马大定理

方程 $x^n+y^n=z^n$（$n\geqslant 3$ 为正整数）无正整数解 (x, y, z).

费马大定理已于 1994 年 6 月被普林斯顿大学数学教授 A. Wiles（外尔斯）完全解决. 至此，这一困扰人们近四百年的世界性难题终于脱去了神秘的面纱，露出了庐山真面目.

【典型例题与基本方法】

1. 因式分解法

将方程的一边化为常数，作素因数分解，另一边含未知数的代数式也因式分解，再考虑各因式的取值，分解成若干个方程（组）来求解.

例 1 求所有的有理数 r，使得方程

$$rx^2+(r+1)x+(r-1)=0 \qquad ①$$

的所有解都是整数.

解 当 $r=0$ 时，方程为 $x-1=0$，它的根 $x=1$ 是整数.

当 $r\neq 0$ 时，方程①是一个关于 x 的一元二次方程，若它有整根 x_1，x_2（不妨设 $x_1\geqslant x_2$），由韦达定理，得

$$\begin{cases} x_1+x_2=-1-\dfrac{1}{r}, \\ x_1x_2=1-\dfrac{1}{r}, \end{cases}$$

从中消去 r，得 $x_1x_2-x_1-x_2=2$，即 $(x_1-1)(x_2-1)=3$.

由此可得

$$\begin{cases} x_1-1=3, \\ x_2-1=1, \end{cases} \quad \begin{cases} x_1-1=-1, \\ x_2-1=-3, \end{cases}$$

解得 $x_1=4$，$x_2=2$ 或 $x_1=0$，$x_2=-2$. 从而求得 $r=-\dfrac{1}{7}$ 或 1.

综上所述，当 $r=0$ 或 $\frac{1}{7}$ 或 1 时，方程①的所有根均为整数.

例 2 求不定方程 $\frac{1}{2}(x+y)(y+z)(z+x)+(x+y+z)^3=1-xyz$ 的整数解.

解 作代换，设 $x+y=u$，$y+z=v$，$z+x=w$，则原方程变形为

$$4uvw+(u+v+w)^3=8-(u+v-w)(u-v+w)(-u+v+w),$$

展开后，合并同类项，得

$$4(u^2v+v^2w+w^2u+uv^2+vw^2+wu^2)+8uvw=8,$$

即 $$u^2v+v^2w+w^2u+uv^2+vw^2+wu^2+2uvw=2.$$

对上式左边进行因式分解，得 $(u+v)(v+w)(w+u)=2$.

于是 $(u+v,v+w,w+u)=(1,1,2),(-1,-1,2),(-2,-1,1)$ 及对称的情形，分别求解，可得 $(u,v,w)=(1,0,1),(1,-2,1),(-1,0,2)$，进而 $(x,y,z)=(1,0,0),(2,-1,-1)$.

综上所述，结合对称性，可知原方程的整数解为 $(x,y,z)=(1,0,0),(0,1,0),(0,0,1),(2,-1,-1),(-1,2,-1),(-1,-1,2)$，共 6 组解.

例 3 求所有满足方程 $2x^2+5y^2=11(xy-11)$ 的正整数数组 (x,y).

解 移项，因式分解，得 $(2x-y)(x-5y)=-121$.

于是 $\begin{cases}2x-y=-121,\ -11,\ -1,\ 1,\ 11,\ 121,\\ x-5y=1,\ 11,\ 121,\ -121,\ -11,\ -1,\end{cases}$

其中仅有方程组 $\begin{cases}2x-y=1,\\ x-5y=-121\end{cases}$ 导出一组正整数解为 $(x,y)=(14,27)$.

例 4 求所有的三元正整数组 (x,y,z)，使得 y 为素数，且 3 和 y 都不是 z 的约数，并满足 $x^3-y^3=z^2$.

解 由原方程得 $z^2=(x-y)(x^2+xy+y^2)$.

设 $(x-y,x^2+xy+y^2)=(x-y,(x-y)^2+3xy)=(x-y,3xy)=(x-y,3y^2)=d$，则 $d\mid 3y^2$. 由 y 为素数及 3 与 y 都不是 z 的约数，可知 $d=1$. 于是 $x-y$，x^2+xy+y^2 都是完全平方数，我们设

$$\begin{cases}x-y=u^2, & ①\\ x^2+xy+y^2=v^2, & ②\end{cases}$$

这里 $u,v\in\mathbf{N}^*$，对方程②两边乘以 4，配方，移项并分解因式，得

$$(2v-2x-y)(2v+2x+y)=3y^2,$$

注意到 y 为素数，并且 $2v+2x+y\in\mathbf{N}^*$，以及 $2v-2x-y<2v+2x+y$，因此

$$\begin{cases}2v-2x-y=1,\ y,\ 3,\\ 2v+2x+y=3y^2,\ 3y,\ y^2.\end{cases}$$

对第1种情形，两式相减，得 $3y^2-1-2(2x+y)-4u^2+6y$.

于是 $u^2+1\equiv 0 \pmod 3$，但 $u^2\equiv 0$ 或 $1 \pmod 3$，此时无解.

对第2种情形，则有 $2y=4x+2y$，导出 $x=0$，亦无解.

对第3种情形，可知 $y^2-3=4u^2+6y \Rightarrow (y-2u-3)(y+2u-3)=12$，

解得 $(y,u)=(7,1)$，进而 $(x,z)=(8,13)$.

故原方程的正整数解为 $(x,y,z)=(8,7,13)$.

2. 配方法

将已知方程变形为一边是平方和的形式，另一边是常数，从而求得方程的整数解或判定方程无解的方法叫做配方法.

例5 求不定方程 $x^2(y-1)+y^2(x-1)=1$ 的整数解.

解 设 (x,y) 为方程的整数解，并设 $x\leqslant y$，则 $y\geqslant x$，这时，将原方程视为 x 的一元二次方程 $(y-1)x^2+y^2\cdot x-(y^2+1)=0$. ①

方程①有整数解，于是 $\Delta=y^4+4(y-1)(y^2+1)$ 是一个完全平方数，即

$(y^2+2y)^2-8y^2+4y-4$

为完全平方数.

注意到当 $y\geqslant 8$ 时，$(y^2+2y-3)^2>\Delta>(y^2+2y-4)^2$，而当 $2<y<8$ 时，有 $(y^2+2y-2)^2>\Delta>(y^2+2y-3)^2$，从而 $y>2$ 时，Δ 都不是完全平方数，所以 $y=2$，进而 $x=1$ 或 -5.

综上，方程的整数解 $(x,y)=(1,2),(2,1),(-5,2)$ 或 $(2,-5)$.

例6 证明：不定方程 $x^2+y^2+z^2+3(x+y+z)+5=0$ 没有有理数解.

证明 将方程两边乘以4，配方，得

$(2x+3)^2+(2y+3)^2+(2z+3)^2=7$.

此方程有有理数解的充要条件是：方程 $a^2+b^2+c^2=7m^2$ ①

有整数解 (a,b,c,m)，并且其中 $m\in\mathbf{N}^*$.

如果①有整数解 (a,b,c,m)，$m\in\mathbf{N}^*$. 我们设 m 是所有这样的解中最小的正整数.

若 m 为偶数，则 $a^2+b^2+c^2\equiv \pmod 4$，注意到，完全平方数 $\equiv 0$ 或 $1 \pmod 4$，故 a，b，c 都为偶数. 这表明 $\left(\frac{a}{2},\frac{b}{2},\frac{c}{2},\frac{m}{2}\right)$ 也是①的满足条件的解，与 m 的最小性矛盾.

若 m 为奇数，则 $a^2+b^2+c^2=7m^2\equiv 7 \pmod 8$，但是，完全平方数 $\equiv 0$ 或 $1 \pmod 4$，从而由 $a^2+b^2+c^2\equiv 3 \pmod 4$，可知 a，b，c 都是奇数，这导致 $a^2+b^2+c^2\equiv 3 \pmod 8$，矛盾.

所以，①没有满足条件的整数解，从而原方程没有有理数解.

3. 不等式估计法

例 7 求所有的整数数组 (a,b,c,x,y,z)，使得

$$\begin{cases}a+b+c=xyz,\\ x+y+z=abc.\end{cases}$$

这里 $a\geqslant b\geqslant c\geqslant 1$，$x\geqslant y\geqslant z\geqslant 1$.

解 由对称性，我们只需考虑 $x\geqslant a$ 的情形. 这时，$xyz=a+b+c\leqslant 3a\leqslant 3x$，故 $yz\leqslant 3$. 于是，$(y,z)=(1,1),(2,1),(3,1)$.

当 $(y,z)=(1,1)$ 时，$a+b+c=x$ 且 $x+2=abc$，于是 $abc=a+b+c+2$. 如果 $c\geqslant 2$，则 $a+b+c+2\leqslant 3a+2\leqslant 4a\leqslant abc$，等号当且仅当 $a=b=c=2$ 时成立；如果 $c=1$，则有 $ab=a+b+3$，即 $(a-1)(b-1)=4$，得 $(a,b)=(5,2)$ 或 $(3,3)$.

当 $(y,z)=(2,1)$ 时，$2abc=2x+6=a+b+c+6$，与上类似讨论可知 $c=1$，进而 $(2a-1)(2b-1)=15$，得 $(a,b)=(3,2)$.

当 $(y,z)=(3,1)$ 时，$3abc=3x+12=a+b+c+12$，可知，没有使 $x\geqslant a$ 的解.

综上所述，可知 $(a,b,c,x,y,z)=(2,2,2,6,1,1),(5,2,1,8,1,1),(3,3,1,7,1,1),(3,2,1,3,2,1),(6,1,1,2,2,2),(8,1,1,5,2,1)$ 和 $(7,1,1,3,3,1)$.

例 8 试求方程 $x^2+x=y^4+y^3+y^2+y$ 的整数解.

解 方程两边乘 4，并对左边配方，得

$$(2x+1)^2=4(y^4+y^3+y^2+y)+1. \qquad ①$$

而①的右边 $=(2y^2+y+1)^2-y^2+2y=(2y^2+y)^2+3y^2+4y+1$.

从而当 $y>2$ 或 $y<-1$ 时，有 $(2y^2+y)^2<(2x+1)^2<(2y^2+y+1)^2$.

由于 $2y^2+y$，$2y^2+y+1$ 是两个连续的整数，故它们之间不会含有完全平方数，从而上式不成立，因此 $-1\leqslant y\leqslant 2$. 由此得原方程的全部整数解是

$(x,y)=(0,-1),(-1,-1),(0,0),(-1,0),(-6,2),(5,2)$.

例 9 试求出所有的正整数 a，b，c，其中 $1<a<b<c$，且使得 $(a-1)(b-1)\cdot(c-1)$ 是 $abc-1$ 的约数.

解 令 $x=a-1$，$y=b-1$，$z=c-1$，则 $1\leqslant x<y<z$. 又因为

$$z\leqslant\frac{(x+1)(y+1)(z+1)-1}{xyz}<\frac{(x+1)(y+1)(z+1)}{xyz}$$

$$=\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right)\left(1+\frac{1}{z}\right)\leqslant\left(1+\frac{1}{1}\right)\left(1+\frac{1}{2}\right)\left(1+\frac{1}{3}\right)=4,$$

所以 $\dfrac{(x+1)(y+1)(z+1)-1}{xyz}=2$ 或 3.

(1) 若上式为 2，则 $\dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}+\dfrac{1}{xy}+\dfrac{1}{yz}+\dfrac{1}{zx}=1.$ ①

显然 $x\neq1$. 若 $x\geqslant3$，则 $y\geqslant4$，$z\geqslant5$，从而

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{xy}+\frac{1}{yz}+\frac{1}{zx}\leqslant\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{12}+\frac{1}{20}+\frac{1}{15}=\frac{59}{60}<1,$$

与①式矛盾. 因此，$x=2$，此时，

$$\frac{1}{y}+\frac{1}{z}+\frac{1}{2y}+\frac{1}{yz}+\frac{1}{2z}=\frac{1}{2}.$$

易知 $3\leqslant y\leqslant5$（当 $y\geqslant6$ 时，$z\geqslant7$，上式不成立），仅当 $y=4$ 时，$z=14$ 为整数，故①仅有一组正整数解 (2，4，14).

(2) 若 $(x+1)(y+1)(z+1)/xyz=3$，则

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{xy}+\frac{1}{yz}+\frac{1}{zx}=2. \qquad ②$$

于是 $x=1\left(\text{否则，②式左端}\leqslant\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{6}+\frac{1}{12}+\frac{1}{8}<2\right)$，②式即为

$$\frac{2}{y}+\frac{2}{z}+\frac{1}{yz}=1.$$

易知 $2\leqslant y\leqslant3$，仅当 $y=3$ 时，$z=7$ 为整数.

故满足②式的正整数解为 $(x,y,z)=(1,3,7)$.

综上可知，满足题意的正整数 (a,b,c) 为 $(3,5,15)$，$(2,4,8)$.

4. 构造法

构造法是通过恒等式来证明不定方程有解或者有无穷多组解.

例 10 求所有的整数 a，使方程

$$x^2+axy+y^2=1 \qquad ①$$

有无穷多组整数解 (x,y). 证明你的结论.

解 当 $a=0$ 时，方程为 $x^2+y^2=1$，仅有 4 组解.

若 $a\neq0$，则 (x,y) 为方程①的解的充要条件是：$(x,-y)$ 为方程 $x^2-axy+y^2=1$ 的解. 所以，只需讨论 $a<0$，且方程①有无穷多组非负整数解 (x,y) 的情形.

如果 $a=-1$，则①为 $x^2-xy+y^2=1$，两边乘以 4，再配方得 $(2x-y)^2+3y^2=4$，仅有两组非负整数解.

如果 $a<-1$，注意到 $(-a,1)$ 为①的一组正整数解. 一般地，设 (x,y) 为①的正整数解，且 $x>y$，则 $(x,-ax+y)$ 也是①的解（这一个解，在视①为关于 y 的一元二次方程时，利用韦达定理可得），当然 $(-ax+y,x)$（满足 $-ax+y>x>y$）也是①的正整数解，依此递推，可知这时①有无穷多组正整数解.

综上所述，当 $|a|>1$ 时，方程①有无穷多组整数解；而 $|a|\leqslant1$ 时，①仅有有限组整数解.

例 11 证明：每一个有理数都可以表示为 4 个有理数的立方和.

证明 利用下述恒等式

$$6n=(n+1)^3-n^3-n^3+(n-1)^3$$

可知，对任意的 $n\in\mathbf{Z}$，$6n$ 可以表为 4 个整数的立方和，于是有

$$\frac{q}{p}=\frac{6^3p^2\cdot q}{(6p)^3}=\frac{6n}{(6p)^3}=\left(\frac{n+1}{6p}\right)^3+\left(\frac{-n}{6p}\right)^3+\left(\frac{-n}{6p}\right)^3+\left(\frac{n-1}{6p}\right)^3.$$

这里 $n=6^2p^2q$，所以命题成立.

例 12 （IMO－43 预选题）是否存在正整数 m，使得方程 $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}=\frac{m}{a+b+c}$ 有无穷多组正整数解 (a, b, c)？

解 存在.

如果 $a=b=1$，则 $m=12$. 令

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}-\frac{12}{a+b+c}=\frac{p(a,b,c)}{abc(a+b+c)},$$

其中 $p(a,b,c)=a^2(b+c)+b^2(c+a)+c^2(a+b)+a+b+c-9abc$.

假设 (x,a,b) 是满足 $p(x,a,b)=0$ 的一组解，且 $x<a<b$，由于 $p(x,a,b)=0$ 是关于 x 的二次方程，所以，$y=\frac{ab+1}{x}>b$ 是其另外的一个解.

设 $a_0=a_1=a_2=1$，定义 $a_{n+2}=\frac{a_na_{n+1}+1}{a_{n-1}}$ $(n\geqslant1)$.

我们证明下面的结论：

(1) $a_{n-1}\mid(a_na_{n+1}+1)$；

(2) $a_n\mid(a_{n-1}+a_{n+1})$；

(3) $a_{n+1}\mid(a_{n-1}a_n+1)$.

其中 a_{n-1}，a_n，a_{n+1} 为正整数.

当 $n=1$ 时，以上三个结论显然成立. 假设 $n=k$ 时，以上三个结论也成立.

由 (1) 得 $a_{k-1}\mid(a_ka_{k+1}+1)$，即 a_{k-1} 与 a_k 互素，且 $a_{k-1}\mid[(a_ka_{k+1}+1)a_{k+1}+a_{k-1}]$；

由 (2) 得 $a_k\mid(a_{k-1}+a_{k+1})$，且 $a_k\mid(a_ka_{k+1}^2+a_{k+1}+a_{k-1})$，所以

$a_ka_{k-1}\mid(a_ka_{k+1}^2+a_{k+1}+a_{k-1})$，即 $a_k\left|\left(a_{k+1}\cdot\frac{a_ka_{k+1}+1}{a_{k-1}}+1\right)\right.=a_{k+1}a_{k+2}+1$.

于是，当 $n=k+1$ 时，(1) 也成立.

同理，由于 a_{k-1} 与 a_{k+1} 也互素，且 $a_{k-1}\mid(a_ka_{k+1}+1+a_ka_{k-1})$，由 (3) 得 $a_{k+1}\mid(a_{k-1}a_k+1)$，且 $a_{k+1}\mid(a_{k-1}a_k+1+a_ka_{k+1})$. 所以

$a_{k-1}a_{k+1}\mid[a_k(a_{k-1}+a_{k+1})+1]$，即 $a_{k+1}\mid\left(a_k+\dfrac{a_ka_{k+1}+1}{a_{k-1}}\right)=a_k+a_{k+2}$.

于是，当 $n=k+1$ 时，(2) 也成立.

由 a_{k+2} 的定义及 (1) 知 a_{k+2} 是整数，且 $a_{k+2}\mid(a_ka_{k+1}+1)$.

于是，当 $n=k+1$ 时，(3) 也成立.

从而可得数列 $\{a_n\}$，当 $n\geqslant2$ 时严格递增，且 $p(a_n,a_{n+1},a_{n+2})=0$，即 (a_n,a_{n+1},a_{n+2}) 是原方程的解，$\{a_n\}=\{1,1,1,2,3,7,11,26,41,97,153,\cdots\}$.

例 13 （1999 年保加利亚第四轮竞赛题）方程 $x^3+y^3+z^3+t^3=1999$ 有无穷多组整数解.

解 注意到 $10^3+10^3+0^3+(-1)^3=1999$. 令 $x=10-k$，$y=10+k$，$z=m$，$t=-1-m$，这里 k，$m\in\mathbf{Z}$，代入原方程，化简可知 k，m 满足 $m(n+1)=20k^2$，即

$$(2m+1)^2-80k^2=1. \qquad ①$$

这是一个 Pell 方程，且 $m=4$，$k=1$ 是 Pell 方程的一个解，并且方程的所有正整数解 (m_n,k_n) 满足

$$(2m_n+1)+k_n\sqrt{80}=(9+\sqrt{80})^n.$$

这样的 (m_n,k_n) 有无穷多对，故原方程有无穷多组整数解.

注 适当地变量代换后，化为熟知的不定方程，转化问题. 本题转化为 Pell 方程后，利用了 Pell 方程的通解公式.

5. 同余方法

如果不定方程 $F(x_1,x_2,\cdots,x_n)$ 有整数解，则对任意 $m\in\mathbf{N}^*$，其整数解 $(x_1,\cdots,x_n)$ 均满足

$$F(x_1,\cdots,x_n)\equiv0\pmod m. \qquad (*)$$

运用这一条件，同余方程 (*) 有解即为原方程有解的一个必要条件. 另外，也可用同余的方法排除一些情形，使不定方程的求解得以简化.

例 14 （2003 年国家集训队试题）正整数 n 不能被 2，3 整除，且不存在非负整数 a，b，使得 $|2^a-3^b|=n$. 求 n 的最小值.

解 $n=1$ 时，$|2^1-3^1|=1$；$n=5$ 时，$|2^2-3^2|=5$；$n=7$ 时，$|2^1-3^2|=7$；$n=11$ 时，$|2^4-3^3|=11$；$n=13$ 时，$|2^4-3^1|=13$；$n=17$ 时，$|2^6-3^4|=17$；$n=19$ 时，$|2^3-3^3|=19$；$n=23$ 时，$|2^5-3^2|=23$；$n=25$ 时，$|2^1-3^3|=25$；$n=29$ 时，$|2^5-3^1|=29$；$n=31$ 时，$|2^5-3^0|=31$.

下证 $n=35$ 满足要求，用反证法.

若不然，存在非负整数 a，b 使得 $|2^a-3^b|=35$.

(1) 若 $2^a-3^b=35$，显然 $a\neq0$，1，2，故 $a\geqslant3$，模 8，得 $-3^b\equiv3\pmod 8$，即

$3^b\equiv5 \pmod 8$，但 $3^b\equiv1,3 \pmod 8$，不可能.

(2) 若 $3^b-2^a=35$，易知 $b\neq0$，1，模 9，得 $2^a\equiv1 \pmod 9$.

而 $\{2^k \pmod 9\}$：$2,4,8,7,5,1,2,4,\cdots$，即

$2^{6k}\equiv1 \pmod 9$，$2^{6k+1}\equiv2 \pmod 9$，$2^{6k+2}\equiv4 \pmod 9$，

$2^{6k+3}\equiv8 \pmod 9$，$2^{6k+4}\equiv7 \pmod 9$，$2^{6k+5}\equiv5 \pmod 9$.

于是 $a=6k$，k 为非负整数，所以 $3^b-8^{2k}=35$.

再模 7，得 $3^b\equiv1 \pmod 7$，而 $\{3^k \pmod 7\}$：3，2，6，4，5，1，3，2，…，故 $b=6k'$，k'为正整数，所以 $3^{6k'}-2^{6k}=35$，即 $(3^{3k'}-2^{3k})(3^{3k'}+2^{3k})=35$，

因此，$\begin{cases}3^{3k'}-2^{3k}=1,\\3^{3k'}+2^{3k}=35,\end{cases}$ 或 $\begin{cases}3^{3k'}-2^{3k}=5,\\3^{3k'}+2^{3k}=7.\end{cases}$

于是，$3^{3k'}=18$ 或 6，不可能.

综上，所求的最小的 n 为 35.

例 15 求不定方程 $1+5^x=2^y+2^z\cdot5^t$ 的正整数解 (x,y,z,t).

解 设 (x,y,z,t) 是原方程的正整数解.

对方程两边模 5，就有 $2^y\equiv1 \pmod 5$，由于 2 是模 5 的原根，故 $4|y$. 这时，对方程两边模 4，可知 $2^z\equiv2 \pmod 4$，所以 $z=1$.

我们设 $y=4r$，得 $5^x-2\cdot5^t=16^r-1$. ①

上式两边模 3，应有 $(-1)^x-(-1)^{t+1}\equiv0 \pmod 3$，故 $x\equiv t+1 \pmod 2$. 进一步，两边模 8，得 $5^x\equiv2\cdot5^t-1\equiv1 \pmod 8$ [这里用到 $5^t\equiv5$ 或 $1 \pmod 8$]，于是 x 为偶数，t 为奇数.

注意到，若 $t=1$，则 $5^x=16^r+9$，设 $x=2m$，就有 $(5^m-3)(5^m+3)=16^r$，由于 $(5^m-3,5^m+3)=(5^m-3,6)=2$，于是，只能是 $5^m-3=2$，$5^m+3=2^{4r-1}$，从而 $m=1$，$r=1$；若 $t>1$，则 $5^3|5^x-2\cdot5^t$，进而 $5^3|16^r-1$，由二项式定理，展开 $16^r-1=(15+1)^r-1$，可知 $5|r$，于是，设 $r=5k$，就有 $16^r-1=16^{5k}-1\equiv(5^5)^k-1\equiv(5\times3^2)^k-1\equiv0 \pmod{11}$. 这要求 $11|5^x-2\cdot5^t$，故 $11|5^{x-t}-2$，但是，对任意 $m\in\mathbf{N}^*$，均有 $5^m\equiv5$，3，4，9 或 $1 \pmod{11}$，不可能出现 $5^{x-t}\equiv2 \pmod{11}$ 的情形，矛盾.

综上所述，方程有唯一解 $(x,y,z,t)=(2,4,1,1)$.

例 16 求所有满足方程

$$8^x+15^y=17^z \quad ①$$

的三元正整数组 $(x、y、z)$.

解 在①式两边取 mod 8 得 $(-1)^y\equiv1 \pmod 8$，所以 y 是偶数，再 mod 7 得 $2\equiv3^z \pmod 7$，所以 z 也是偶数.

此时，令 $y=2m$，$z=2t(m,t\in\mathbf{N})$.

于是，由①式可知：$2^{3x}=(17^t-15^m)(17^t+15^m)$.

由唯一分解定理：$17^t-15^m=2^s$，$17^t+15^m=2^{3x-s}$，从而

$$17^t=\frac{1}{2}(2^s+2^{3x-s})=2^{s-1}+2^{3x-s-1}. \qquad ②$$

注意到 17 是奇数，所以要使②式成立，一定有 $s=1$，于是

$$17^t-15^m=2. \qquad ③$$

当 $m\geqslant 2$ 时，在③式两边 mod 9 得 $(-1)^t\equiv 2(\mathrm{mod}\,9)$，这显然是不成立的，所以 $m=1$，从而 $t=1$，$x=2$. 故方程①只有唯一一组正整数解 $(x,y,z)=(2,2,2)$.

注 处理这类"指数型"的不定方程，一个常用的办法就是取模. 这样就能利用同余的性质导出解或与之相关的量所满足的一些性质（比如奇偶性），使问题简化. 这种方法的关键是选一个好的模，使取模之后真正能得到一些关系. 这样就要求因取模而进行的同余运算是简单的. 就本题而言，第一次取 mod 8，就是因为 $15\equiv -1(\mathrm{mod}\,8)$，$17\equiv 1(\mathrm{mod}\,8)$ 的缘故.

6. 无穷递降法

数学竞赛中，经常出现一些用无穷递降法来解的竞赛题，那么什么是无穷递降法呢?

从本质上讲，无穷递降法是一种用反证法表现的特殊形式的数学归纳法，它首先由 Fermat 创立并运用它证明了方程 $x^4+y^4=z^4$ 没有非零整数解. 从此，无穷递降法作为一种重要的思想方法广为流传，并在数论、平面几何、图论及组合中经常用到它.

例 17 设 $p\equiv -1(\mathrm{mod}\,4)$ 是一个素数. 证明：对任意的 $n\in\mathbf{N}^*$，方程

$$p^n=x^2+y^2 \qquad ①$$

没有正整数解.

证明 设 n 是使方程①有正整数解中最小的数. 我们的目标是证明有比 n 更小的数使①有正整数解，从而导出矛盾. 为此设 (x_0,y_0) 是方程①的一组解，则 $(x_0,y_0)=1$［否则有 $(x_0,y_0)=p^l$，从而方程 $p^{n-2l}=x^2+y^2$ 有正整数解 $\left(\frac{x_0}{p^l},\frac{y_0}{p^l}\right)$，矛盾］，并且 n 为偶数，这是因为：由 $(x_0,y_0)=1$ 及①知，x_0，y_0 为一奇一偶，从而

$p_n\equiv(-1)^n\equiv x_0^2+y_0^2\equiv 1(\mathrm{mod}\,4)$，故 n 为偶数.

设 $n=2n_1(n_1\geqslant 1)$，由方程①得 $(p^{n_1})^2=x_0^2+y_0^2$.

即 (x_0,y_0,p^{n_1}) 是一组本原勾股数. 结合勾股数方程的知识，可知存在正整数 a,b，$(a,b)=1$，使得

$$p^{n_1}=a^2+b^2.$$

这表明方程 $p^{n_1}=x^2+y^2$ 有正整数解，而 $n_1=\frac{n}{2}<n$，这与 n 的最小性矛盾.

注 用无穷递降法证明不定方程无正整数解的重要步骤是：假设存在一组正整数解，设法造出这个方程的另一组正整数解，而新的解比原来的解"严格地小". 由上面的过程可以无限进行下去，则由于严格递减的正整数数列只有有限项，从而导出矛盾. 也可以假设正整数解中的一组"最小"的解，通过递降得到一组新的"更小"的解，由此产生矛盾.

例 18 （IMO-29 试题）已知正整数 a 和 b，使得 $ab+1$ 整除 a^2+b^2，求证：$\frac{a^2+b^2}{ab+1}$是某个正整数的平方.

分析 实际上是讨论二次方程 $a^2+b^2=k(ab+1)$（将 k 看成常数）的解存在与否的问题. 由于是二次方程，我们可以使用韦达定理，由方程的一组解产生出另一组解，再结合无穷递降法与最小数原理，便不难把它的解的情况讨论清楚.

证明 我们只需证明，当 k 不是完全平方数时，关于 a，b 的不定方程

$$a^2+b^2=k(ab+1) \quad ①$$

没有正整数解 (a,b).

采用反证法. 反设①有正整数解（k 不为完全平方数时），则可以从①的所有正整数解 (a,b) 中选出使 $\min\{a,b\}$ 最小的一组解，设为 (a_0,b_0)，并不妨设 $a_0\geqslant b_0$.

先证 $k<b_0^2$ 且 $a_0<kb_0$. ②

反证法. 反设 $k>b_0^2$（$k\neq b_0^2$），则

$a_0(a_0-kb_0)=k-b_0^2$，

于是 $a_0-kb_0>0$，且 $a_0\leqslant k-b_0^2$（因为 $a_0\mid k-b_0^2$），这两个不等式显然不能同时成立，矛盾. 故②的两不等式成立.

考虑一元二次方程 $x^2-kb_0x+b_0^2-k=0$. 它的一个根为 $a_0\in\mathbf{Z}^+$，不妨设另一根为 a_1，则由韦达定理

$$\begin{cases}a_0+a_1=kb_0, & ③\\ a_0a_1=b_0^2-k. & ④\end{cases}$$

利用②③可知 $a_1\in\mathbf{Z}^+$，且 $a_1=\frac{b_0^2-k}{a_0}<\frac{b_0^2}{a_0}\leqslant b_0$.

于是我们得到了①另一组正整数解 (a_1,b_0)，$\min\{a_1,b_0\}=a_1<b_0=\min\{a_0,b_0\}$，这与我们假定 $\min\{a_0,b_0\}$ 最小相矛盾.

从而反设不成立.

∴当 k 不是完全平方数时，①并无正整数解（a，b）.

【解题思维策略分析】

例 19 （IMO－44 试题）求所有的正整数对（a，b），使得 $\frac{a^2}{2ab^2-b^3+1}$ 是一个正整数.

解法 1 设（a，b）为满足条件的正整数对，由于

$$k=\frac{a^2}{2ab^2-b^3+1}>0,$$

故 $2ab^2-b^3+1>0$，$a>\frac{b}{2}-\frac{1}{2b^2}$，因此 $a\geqslant\frac{b}{2}$，结合 $k\geqslant1$，因此有

$$a^2\geqslant b^2(2a-b)+1,$$

从而 $a^2>b^2(2a-b)\geqslant0$. 所以 $a>b$ 或者 $2a=b$. ①

现设 a_1，a_2 为关于 a 的方程（k，b 固定）

$$a^2-2kb^2a+k(b^3-1)=0 \quad ②$$

的两个解，且其中之一是一个整数，则由 $a_1+a_2=2kb^2$ 可知另一个解也是整数，不妨设 $a_1\geqslant a_2$，则 $a_1\geqslant kb^2>0$，进一步，由 $a_1a_2=k(b^3-1)$，得

$$0\leqslant a_2=\frac{k(b^3-1)}{a_1}\leqslant\frac{k(b^3-1)}{kb^2}<b,$$

利用①可知 $a_2=0$ 或者 $a_2=\frac{b}{2}$（此时 b 为偶数）.

若 $a_2=0$，则 $b^3-1=0$，因此 $a_1=2k$，$b=1$.

若 $a_2=\frac{b}{2}$，则 $k=\frac{b^2}{4}$，$a_1=\frac{b^4}{2}-\frac{b}{2}$.

综上可知，只能是$(a,b)=(2l,1),(l,2l)$或者$(8l^4-l,2l)$，其中 l 为正整数，直接验证，可知上述形式的(a,b)符合题意.

解法 2 当 $b=1$ 时，由条件知 a 为偶数.

当 $b>1$ 时，我们记 $\frac{a^2}{2ab^2-b^3+1}=k$，则关于 a 的一元二次方程②有正整数解，从而关于 a 的判别式为完全平方数，即 $\Delta=4k^2b^4-4k(b^3-1)$是完全平方数.

注意到，当 $b\geqslant2$ 时，我们有

$$(2kb^2-b-1)^2<\Delta<(2kb^2-b+1)^2. \quad ③$$

上述式子可以这样来证明：

$$\Delta-(2kb^2-b-1)^2=4kb^2-b^2\quad 2b+4k-1=(4k-1)(b^2+1)-2b$$
$$\geqslant2(4k-1)b-2b>0;$$
$$(2kb^2-b+1)^2-\Delta=4kb^2\quad 4k-(b-1)^2=4k(b^2-1)-(b-1)^2$$

$>(4k-1)(b^2-1)>0.$

所以，③式成立.

利用 Δ 为完全平方数及③式，可知

$\Delta=4k^2b^4-4k(b^3-1)=(2kb^2-b)^2$，

于是，$4k=b^2$，进而 b 为偶数. 设 $b=2l$，则 $k=l^2$，利用②可求得 $a=l$ 或 $8l^4-l$.

综上，满足条件的 $(a,b)=(2l,1),(l,2l)$ 或 $(8l^4-l,2l)$，其中 l 为正整数，直接验证，可知它们符合要求.

例 20 数列 $\{u_n\}_{n=0}^{\infty}$ 满足

$u_0=0$，$u_1=1$，$u_{n+2}=2u_{n+1}-pu_n$，$n=0,1,2,\cdots$， ①

其中 p 是一个奇素数（素数即质数）. 证明：当且仅当 $p=5$ 时，数列 $\{u_n\}$ 中存在某一项 u_k，使 $u_k=-1$.

解 在①式两边取 mod p 得 $u_{n+2}\equiv 2u_{n+1}\pmod p$，反复利用这个式子，我们有：

$u_n\equiv 2^{n-1}\pmod p$，$n=1,2,\cdots$ ②

再取 mod $p-1$ 得：

$u_{n+2}\equiv 2u_{n+1}-u_n\pmod{p-1}$，即

$u_{n+2}-u_{n+1}\equiv u_{n+1}-u_n\pmod{p-1}$.

从而 $u_{n+2}-u_{n+1}\equiv u_{n+1}-u_n\equiv u_n-u_{n-1}\equiv\cdots\equiv u_1-u_0\equiv 1\pmod{p-1}$.

所以 $u_n\equiv\sum\limits_{j=1}^{n}(u_j-u_{j-1})\equiv n\pmod{p-1}$. ③

如果数列 $\{u_n\}$ 中存在某项 u_k，使 $u_k=-1$，在②，③中，令 $n=k$，我们得到：

$2^{k-1}\equiv -1\pmod p$， ④

$k\equiv -1\pmod{p-1}$. ⑤

利用费马小定理 $2^{p-1}\equiv 1\pmod p$ 及④，有：

$2^{k+1}\equiv 1\pmod p$.

再结合③便有

$2^{k-1}\cdot 1\equiv(-1)\cdot 2^{k+1}\pmod p$，

即 $1\equiv -4\pmod p$.

从而 $p\mid 5$，所以 $p=5$.

当 $p=5$ 时，直接计算便知 $u_3=-1$，从而原命题得证.

注 对于这个问题，我们的想法是先找出数列 $\{u_n\}$ 中的项所满足的一些性质，看看哪些性质对解决问题有用，然后再从这些性质去考虑.

基于这个想法，我们很容易得到②，于是有④，从④的形式中使我们联想到费马小定理，从而使我们考虑去找 k 和 $p-1$ 的关系，于是才想到①中取 mod $p-1$.

例 21 设 n 是正整数. 证明：不定方程

$$\sum_{j=1}^{n} a_j^3 = \left(\sum_{j=1}^{n} a_j\right)^2 \quad ①$$

仅有一组互不相同的正整数解$\{1,2,\cdots,n\}$.

解 不妨设 $a_1<a_2<\cdots<a_n$. ②

从①式左、右两边次数上的差异，我们可以猜想出 a_n 不可能很大，否则①中的"="将改成">". 经过探索发现，在条件②下，我们可以证明

$$\sum_{j=1}^{n} a_j^3 \geqslant \left(\sum_{j=1}^{n} a_j\right)^2. \quad ③$$

这是因为

$$\begin{aligned}\sum_{j=1}^{n} a_j^3 - \left(\sum_{j=1}^{n} a_j\right)^2 &= \sum_{j=1}^{n} a_j^3 - \sum_{j=1}^{n}\left(a_j^2 + 2a_j\sum_{i=1}^{j-1} a_i\right)\\ &= \sum_{j=1}^{n} 2a_j\left[a_j\frac{(a_j-1)}{2} - \sum_{i=1}^{j-1} a_i\right]\\ &= \sum_{j=1}^{n} 2a_j\left[1+2+\cdots+(a_j-1) - \sum_{i=1}^{j-1} a_i\right].\end{aligned}$$

注意到条件②，可知

$$1+2+\cdots+(a_j-1) \geqslant \sum_{i=1}^{j-1} a_i (j=1,2,\cdots,n),$$

等号仅在 $a_k=k$ 时取得，$k=1, 2, \cdots, j$.

于是，③得证，并知等号成立当且仅当 $a_j=j(j=1,2,\cdots,n)$.

故①仅有一组互不相同的正整数解 $\{1, 2, \cdots, n\}$.

注 宏观的估计，进而猜测，以及不等式的应用是解决这个问题的关键.

例 22 （2002 年全国高中数学联赛题）在世界足球赛前，F 国教练为了考察 A_1，A_2，…，A_7 这七名队员，准备让他们在三场训练比赛（每场 90 分钟）都上场. 假设在比赛的任何时刻，这些队员中有且仅有一人在场上，并且 A_1，A_2，A_3，A_4 每人上场的总时间（以分钟为单位）均被 13 整除. 如果每场换人次数不限，那么按各队员上场的总时间计算，共有多少种不同的情况?

解 设第 i 名队员上场的时间为 x_i 分钟（$i=1, 2, \cdots, 7$），问题转化为求不定方程 $x_1+x_2+\cdots+x_7=270$ （*）

满足条件 $7|x_i(i=1,2,3,4)$，且 $13|x_j(i=5,6,7)$时正整数解的组数.

设 $x_1+x_2+x_3+x_4=7m$，$x_5+x_6+x_7=13n$，则

$7m+13n=270$，且 m，$n\in\mathbf{N}^+$，$m\geqslant4$，$n\geqslant3$.

容易求得满足上述条件的正整数解（m，n）为

$(m,n)=(33,3),(20,10),(7,17)$.

当$(m,n)=(33,3)$时，$x_5=x_6=x_7=13$. 又设$x_i=7y_i(i=1,2,3,4)$，则$y_1+y_2+y_3+y_4=33$，有$C_{33-1}^{4-1}=C_{32}^3=4960$组正整数解$(y_1,y_2,y_3,y_4)$，此时有4960组满足条件的正整数解.

当$(m,n)=(20,10)$时，令$x_i=7y_i(i=1,2,3,4)$，$x_j=13y_j(j=5,6,7)$，于是，$y_1+y_2+y_3+y_4=20$，$y_5+y_6+y_7=10$，此时(*)有$C_{19}^3\cdot C_9^2=34884$组解.

当$(m,n)=(7,17)$时，令$x_i=7y_i(i=1,2,3,4)$，$x_j=13y_j(j=5,6,7)$，于是$y_1+y_2+y_3+y_4=7$，$y_5+y_6+y_7=17$，此时(*)有$C_6^3\cdot C_{16}^2=2400$组解.

故满足(*)的正整数解为$4960+34884+2400=42244$组.

【模拟实战】

习题A

1. 证明：(1) 方程$x(x+1)+1=y^2$没有正整数解.

   (2) 方程$x(x+1)=y^k$($k\geqslant 2$为正整数)没有正整数解.
2. (1977年匈牙利数学竞赛题) 求证：对任意素数$p>5$，方程$x^4+4^x=p$没有整数解.
3. 设$a,b\in\mathbf{N}^*,(a,b)=1$. 求最小的正整数$c_0$，使得对任意$c\in\mathbf{N}^*$，$c\geqslant c_0$，不定方程$ax+by=c$有非负整数解.
4. 设$a,b\in\mathbf{N}^*,(a,b)=1$. 求所有自然数$c$的个数，使得不定方程$ax+by=c$没有非负整数解.
5. 求不定方程$(a^2-b)(a+b^2)=(a+b)^2$的所有正整数解.
6. 求所有的整数对(x,y)，使得$x^3=y^3+2y^2+1$.
7. 设a,b,c,d都是素数，且$a>3b>6c>12d$，$a^2-b^2+c^2-d^2=1749$. 求$a^2+b^2+c^2+d^2$的所有可能值.
8. 求所有的整数数对(x,y)，使得$x^2+3y^2=1998x$.
9. 证明：不定方程$x^2=y^5-4$没有整数解.
10. 不定方程$x^2+y^2+z^2+u^2+v^2=xyzuv-65$是否存在使$x,y,z,u,v$均大于2000的正整数解?
11. 求满足方程$p(p+1)+q(q+1)=r(r+1)$的所有素数p,q,r.
12. 证明：如果方程$x^7-1=y^2$有正整数解，那么一定有$7\mid y$.
13. 设正整数a,b,n满足$n!=a!\,b!$，证明：$a+b<n+2\log_2 n+4$.

14. 证明：如果方程 $px^2+qy^2=1$（p，$q\in\mathbf{N}$）至少有一组正整数解（x^*，y^*），那么它一定有无穷多组正整数解，其中 pq 不是完全平方数.
15. 证明：若正整数 x，y 使得 $2xy \mid x^2+y^2-x$，则 x 是完全平方数.
16. 证明：若正整数 k，l，m，n 满足 $k<l<m<n$ 及 $kn=lm$，则有不等式
$\left(\frac{n-k}{2}\right)^2\geqslant k+2$.
17.（CMO－20 试题）求方程 $2^x\cdot3^y-5^z\cdot7^w=1$ 的全部非负整数解(x,y,z,w).

习题 B

1.（2003 年国家集训队测试题）正整数 x，y 满足 $x<y$，令 $P=\frac{x^3-y}{1+xy}$，求 P 能取到的所有整数值.
2.（2006 年东南数学奥林匹克题）(1) 求不定方程 $mn+nr+mr=2(m+n+r)$ 的正整数解(m,n,r)的组数；
(2) 对于给定的整数 $k>1$，证明：不定方程 $mn+nr+mr=k(m+n+r)$ 至少有 $3k+1$ 组正整数解(m,n,r).
3.（第 16 届韩国数学奥林匹克题）证明：不存在整数 x，y，z，满足
$2x^4+2x^2y^2+y^4=z^2$，$x\neq0$.
4.（第 17 届北欧数学竞赛题）求所有的三元整数组（x，y，z），使得
$x^3+y^3+z^3-3xyz=2003$.
5.（第 22 届伊朗数学奥林匹克题）求所有的素数 p，q，r，使得等式 $p^3=p^2+q^2+r^2$ 成立.
6.（2004 年日本数学奥林匹克题）求有多少个正整数对（m，n），使得
$7m+3n=10^{2004}$，且 $m\mid n$.
7.（第 21 届巴尔干数学奥林匹克题）已知 x，y 是素数. 求不定方程 $x^2-y^2=xy^2-19$ 的解.
8.（第 20 届韩国数学奥林匹克题）试求所有的三元正整数组（x，y，z），使得
$1+4^x+4^y=z^2$.
9.（2007 年克罗地亚数学竞赛题）求方程 $x^2+11^3=y^3$ 的全部整数解.
10.（2002—2003 年度芬兰高中数学竞赛题）求满足$(n+1)^k-1=n!$ 的所有正整数对(n,k).
11.（2005 年巴尔干数学奥林匹克题）求方程 $3^x=2^xy+1$ 的正整数解.
12.（2005 年捷克-波兰-斯洛伐克数学竞赛题）求满足方程 $y(x+y)=x^3-7x^2+$

$11x-3$的所有整数对(x, y).

13. (2005年克罗地亚数学竞赛题)在正整数集中,求方程$k!\,l!=k!+l!+m!$的所有解.

14. (2004年澳大利亚数学奥林匹克题)求使$(a^3+b)(a+b^3)=(a+b)^4$成立的所有整数对(a,b).

15. (IMO-43预选题)是否存在正整数m,使得方程

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}=\frac{m}{a+b+c}$$

有无穷多组正整数解(a, b, c)?

16. (第57届白俄罗斯数学奥林匹克题)求所有的正整数n,m,满足

$$n^5+n^4=7^m-1.$$

17. (IMO-47预选题)求方程$\frac{x^7-1}{x-1}=y^5-1$的所有整数解.

18. (2004年澳大利亚数学奥林匹克题)求具有如下性质的所有四元实数组(a, b, c, d):

    四个数中的任意三个数的积再与剩下的那个数相加所得的和都是相等的,而与三个数的选择无关.

19. (2005年全国高中数学联赛题)如果自然数a的各位数字之和等于7,那么称a为"吉祥数".将所有"吉祥数"从小到大排成一列a_1,a_2,a_3,…,若$a_n=2005$,则$a_{5n}=$________.

20. (1990年上海市高三数学竞赛题)在区间$1\leqslant n\leqslant 10^6$中,使得方程$n=x^y$有非负整数解$x$,$y$,且$x\neq n$的整数$n$共有多少个?

21. (1995年全国高中数学联赛题)求一切实数p,使得三次方程

$$5x^3-5(p+1)x^2+(71p-1)x+1=66p$$

的三个根均为自然数.

22. (1998年国家集训队选拔考试题)设$f(x)=3x+2$.证明存在正整数m,使得$f^{(100)}(m)$能被1988整除($f^{(k)}(x)$表示$\underbrace{f(f(\cdots f(x)))}_{k个f}$).

23. (1990年国家集训队训练题)设p是素数,证明数列$\left\{\frac{n(n+1)}{2}\right\}$中没有两项之比为$p^{2l}(l\geqslant 1, l, n\in\mathbf{N})$.

24. (1993年国家集训队选拔考试题)试求方程$2x^4+1=y^2$的一切整数解.

25. (2008年国家集训队培训题)设a,b是正整数,满足$(a,b)=1$,a,b不同奇偶.如果集合S具有下面性质:

(1) a，$b\in S$；

(2) 由 x，y，$z\in S$ 可推出 $x+y+z\in S$.

求证：每个大于 $2ab$ 的正整数都属于 S.

26. (2004 年西部数学奥林匹克题) 试求满足 $a^2+b^2+c^2=2005$，且 $a\leqslant b\leqslant c$ 的所有三元正整数组 (a, b, c).

27. (2005 年俄罗斯数学奥林匹克题) 已知正整数 x 和 y 满足 $2x^2-1=y^{15}$. 证明：如果 $x>1$，则 x 可被 5 整除.

28. (2005 年美国数学奥林匹克题) 证明：方程组

$$\begin{cases}x^6+x^3+x^3y+y=147^{157},\\x^3+x^3y+y^2+y+z^9=157^{147}\end{cases}$$

没有整数解.

29. (2005 年俄罗斯数学奥林匹克题) 设正整数 x、y、z ($x>2$，$y>1$) 满足等式 $x^y+1=z^2$. 以 p 表示 x 的不同的素约数的数目，以 q 表示 y 的不同的素约数的数目. 证明：$p\geqslant q+2$.

30. (2007 年西部数学奥林匹克题) 求所有的正整数 n，使得存在非零整数 x_1，x_2，…，x_n，y，满足

$$\begin{cases}x_1+\cdots+x_n=0,\\x_1^2+\cdots+x_n^2=ny^2.\end{cases}$$

31. (2004 年国家集训队选拔考试题) 设 u 为任一给定的正整数，证明方程 $n!=u^a-u^b$ 至多有有限多组正整数解 (n, a, b).

32. (2005 年国家集训队培训题) 试求所有互素的正整数对 (x, y)，使满足：$x\mid y^2+210$，$y\mid x^2+210$.

33. (2005 年国家集训队培训题) (1) 试求所有正整数 k，使得方程

$$a^2+b^2+c^2=kabc \qquad ①$$

有正整数解 (a, b, c)；

(2) 证明：对上述每个 k，方程①都有无穷多个这样的正整数解 (a_n, b_n, c_n)，使得 a_n，b_n，c_n 三数中，任两数之积皆可表示为两个正整数的平方和.

34. (CMO-21 试题) 正整数 m，n，k 满足：$mn-k^2+k+3$，证明不定方程

$$x^2+11y^2=4m \text{ 和 } x^2+11y^2=4n$$

中至少有一个有奇数解 (x, y).

第十八章　整　点

【基础知识】

1. 整点的定义：在平面直角坐标系中，横、纵坐标均为整数的点叫做整点，整点也叫格点.（类似地可定义空间直角坐标系中的整点.）

2. 整点的分类：根据整数的奇偶性可以把整点分为（奇，奇）、（奇，偶）、（偶，奇）、（偶，偶）4类.（类似地空间可分为8类.）

一线段的两端点，如果是一类型的整点，那么这条线段的中点也是整点；反之亦然.

3. 整点多边形的面积公式：顶点都在整点上的简单多边形（即不自交的多边形），其面积为 S，多边形内的整点数为 N，多边形边上的整点数为 L，则

$$S=N+\frac{L}{2}-1.$$

4. 正方形内的整点：

(1) 各边均平行于坐标轴的正方形，如果内部不含整点，它的面积最大是1.

(2) 内部不含整点的正方形面积，最大是2.

(3) 内部只含一个整点的最大正方形面积是4.

5. 圆内整点问题：设 $A(r)$ 表示区域 $x^2+y^2\leqslant r^2$ 上的整点数，r 是正实数，则

$$A(r)=1+4[r]+4\sum_{1\leqslant s\leqslant r}[\sqrt{r^2-s^2}],\text{或}$$

$$A(r)=1+4[r]+8\sum_{1\leqslant s\leqslant\sqrt{2}r}[\sqrt{r^2-s^2}]-4\left[\frac{r}{\sqrt{2}}\right]^2.$$

其中 $[x]$ 表示不超过 x 的最大整数.此外，当 r 充分大时，区域 $x^2+y^2\leqslant r^2$ 上的格点数 $A(r)$ 接近于 πr.

6. 不存在整点正三角形.

7. 当 $n\geqslant5$ 时，不存在整点正 n 边形.

【典型例题与基本方法】

例1　（第30届俄罗斯数学奥林匹克题）能否在平面上的每个整点上都写上1

个正整数，使得三个整点共线，当且仅当写在它们上面的 3 个正整数具有大于 1 的公约数？

解 不能.

假设可以做到. 现考察整点 A，假定它上面写着正整数 a. 设 a 有 n 个不同的素约数.

在平面上再取一个整点 A_1. 显然，在直线 AA_1 上还有别的整点 B_1，例如，可以将 B_1 取为 A 关于 A_1 的对称点.

由于 A，A_1，B_1 上所写的 3 个数有大于 1 的公约数，因此，它们都可以被某个素数 p_1 整除.

特别地，有 $p_1 \mid a$.

再在平面上取一个整点 A_2，使得 A_2 不在直线 AA_1 上.

在直线 AA_2 上还有别的整点 B_2，写在 A，A_2，B_2 上的 3 个数都能被某个素数 p_2 整除.

特别地，有 $p_2 \mid a$.

由于 A，A_1，A_2 三点不共线，所以，$p_1 \neq p_2$，把这一过程持续地做下去，构造出直线 AA_3，AA_4，…，AA_{n+1}，每一次都得到 1 个新的可以整除 a 的素数，一共得到 $n+1$ 个不同的素数，它们都可以整除 a. 此与 a 仅有 n 个不同的素约数的假设相矛盾.

例 2 （IMO－30 预选题）设 L 为平面上所有整点的集合. 证明对 L 中的任意三点 A，B，C，L 中有第四点 D，不同于 A，B，C，使得线段 AD，BD，CD 的内部不含 L 的点，对于 L 中任意四点，结论是否成立？

解 连接整点 $A(a_1,a_2)$，$B(b_1,b_2)$ 的线段内部无整点等价于

$(b_1-a_1,b_2-a_2)=1$.

不妨设已知的三点为 $A(a_1,a_2)$，$B(b_1,b_2)$，$C(0,0)$.

设 $(a_2,b_2)=d$，则

$a_2=a_2'd,b_2=b_2'd,(a_2',b_2')=1$.

由于 $(a_2'-b_2',b_2')=1$，可取整数 s 满足

$sb_2' \equiv 1 \pmod{a_2'-b_2'}$.

令 $y=da_2'b_2's+1$，则

$(y,y-a_2)=(y,y-b_2)=1$.

由于 $b_2's \equiv 1 \pmod{a_2'-b_2'}$，则可设 $b_2's-1=k(a_2'-b_2')$.

$$\begin{aligned}(y-a_2,y-b_2)&=(1+a_2'd(b_2's-1),a_2-b_2)\\&=(1+a_2'dk(a_2'-b_2'),a_2-b_2)\end{aligned}$$

$=(1+a_2'k(a_2-b_2),a_2-b_2)$

$-1.$

由中国剩余定理知，有整数 x 满足不定方程组

$$\begin{cases}x\equiv 1 & (\text{mod } y),\\ x\equiv a_1+1 & (\text{mod } y-a_2),\\ x\equiv b_1+1 & (\text{mod } y-b_2).\end{cases}$$

这里整点 (x,y) 满足

$(x,y)=(x-a_1,y-a_2)=(x-b_1,y-b_2)=1.$

因此存在第四点 D，使得 AD，BD，CD 的内部不含 L 的点.

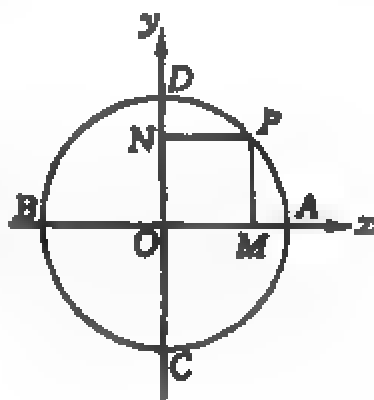
对任意四点，题中所述结论不一定成立.

设集 L 中的四点为

$A(0,0)$，$B(1,0)$，$C(0,1)$，$D(1,1)$.

对于任意一点 $E(x,y)\in L$，则 (x,y) 的奇偶分布情况必与 A，B，C，D 中某一点完全相同，从而 E 与这点的对应的坐标之差均为偶数，连接这点与 E 的线段内部必有整点. 因此，对于 L 中任意四点，题中所述结论不再成立.

例 3 （1982 年全国高中数学联赛题）已知圆 $x^2+y^2=r^2$（r 为奇数）交 x 轴于 $A(r,0)$，$B(-r,0)$，交 y 轴于 $C(0,-r)$，$D(0,r)$. $P(u,v)$ 是圆周上一点，$u=p^m$，$v=q^n$（p，q 都是素数，m，n 都是自然数），且 $u>v$. 点 P 在 x 轴和 y 轴上的射影分别是 M，N.



求证 $|AM|$，$|BM|$，$|CN|$，$|DN|$ 分别为 1，9，8，2.

证法 1 因为 r 为奇数，则由 $u^2+v^2=r^2$ 可得，u 和 v 必一为奇数，一为偶数.

(1) u 为偶数.

因为 $u=p^m$ 为偶数及 p 是素数，所以 $p=2$.

即 $u=2^m$.

$v^2=q^{2n}=r^2-u^2=r^2-(2^m)^2=(r+2^m)(r-2^m).$

因为 q 是素数，所以必有

$$\begin{cases}r-2^m=1,\\ r+2^m=q^{2n}.\end{cases}$$

于是 $r=2^m+1$.

由此可得 $\begin{cases}v^2=2^{m+1}+1=q^{2n},\\ u^2=2^{2m}.\end{cases}$

从而又有$(q^n+1)(q^n-1)=2^{m+1}$.

于是$\begin{cases}q^n+1=2^a,\\ q^n-1=2^b, a>b.\end{cases}$

$2q^n=2^a+2^b$,

$q^n=2^{a-1}+2^{b-1}=2^{b-1}(2^{a-b}+1)$.

因为 q 是奇素数,所以 $2^{b-1}=1, b=1$.

从而 $q^n=2^b+1=3$, 即 $q=3$, $n=1$.

从而 $q^{2n}=q^2=9=2^{m+1}+1$, $m=2$.

于是 $u=4$, $r=5$.

由此得出 $|AM|=1$, $|BM|=9$, $|CN|=8$, $|DN|=2$.

(2) v 为偶数.

同理可得 $u=3$, $v=4$, $r=5$, 但这时与题设中的 $u>v$ 不符.

所以 v 不能为偶数.

由 (1), (2), 本题得证.

证法 2 若 u 为偶数, 则不定方程 $u^2+v^2=r^2$ 可解得

$$\begin{cases}u=2cd,\\ v=c^2-d^2,\\ r=c^2+d^2.\end{cases}$$

因为 $u=p^m=2^m=2cd$, 则可令

$c=2^\alpha$, $d=2^\beta$.

此时 $v=c^2-d^2=(2^\alpha+2^\beta)(2^\alpha-2^\beta)$.

因为 v 是奇数,则 $2^\beta=1,\beta=0$.

从而 $v=q^n=(2^\alpha+1)(2^\alpha-1)$.

又因为 q 是素数,则

$$\begin{cases}2^\alpha+1=q^a,\\ 2^\alpha-1=q^b, a>b.\end{cases}$$

即 $2\cdot 2^\alpha=q^a+q^b=q^b(q^{a-b}+1)$.

由 q 是奇素数可得 $q^b=1, b=0$, 从而有 $2^\alpha=q^b+1=2$, $\alpha=1$, 进而 $q^a=2^\alpha+1=3$, $q=3$, $v=(2^\alpha+1)(2^\alpha-1)=3=q^n, n=1$.

于是可得 $u=4$, $v=3$, $r=5$.

进一步求出 $|AM|=1$, $|BM|=9$, $|CN|=8$, $|DN|=2$.

若 u 为奇数, 同证 1, 不可能.

例 4 (CMO-9 试题) 设 M 为平面上坐标为 ($p\times1994$, $7p\times1994$) 的点, 其

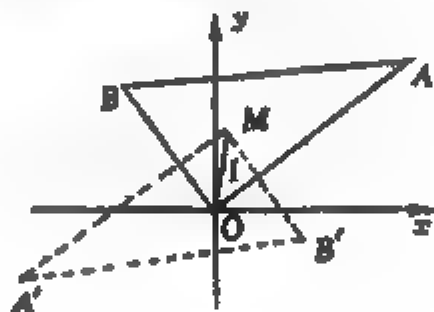
中 p 是素数. 求满足下述条件的直角三角形的个数：

(1) 三角形的三个顶点都是整点，而且 M 是直角顶点；

(2) 三角形的内心是坐标原点.

解 连接坐标原点 O 及点 M，取线段 OM 的中点 $I(p\times 997,7p\times 997)$，把满足条件的一个直角三角形关于点 I 作一个中心对称，即把点(x,y)变换为点$(p\times 1994-x,7p\times 1994-y)$. 于是，满足题目条件的一个整点直角三角形变为一个与之全等的整点直角三角形，三角形的内心变为点 M，直角顶点变为坐标原点. 因此，所求整点直角三角形的个数，只须考虑直角顶点在坐标原点、内心在点 M 的情况即可.

考虑满足上述条件的整点直角$\triangle OAB$.



设$\angle xOA=\alpha$，$\angle xOM=\beta$，则 $\alpha+\frac{\pi}{4}=\beta$.

由题设条件可知 $\tan\beta=7$，

$$\tan\alpha=\tan\left(\beta-\frac{\pi}{4}\right)=\frac{\tan\beta-\tan\frac{\pi}{4}}{1+\tan\beta\tan\frac{\pi}{4}}=\frac{3}{4}.$$

于是直角边 OA 上的任一点的坐标可写成$(4t,3t)$.

由于 A 是整点，若 $A(4t,3t)$，$t\in\mathbf{N}$，则 $OA=5t$.

由$\angle yOB=\alpha$ 可知，B 点的坐标为$(-3t_0,4t_0)$，$t_0\in\mathbf{N}$，$OB=5t_0$.

直角三角形内切圆半径 $r=\frac{\sqrt{2}}{2}OM=5p\times 1994$.

设 $OA=2r+p_0$，$OB=2r+q_0$.

由于 OA，OB，r 都是 5 的倍数，则 p_0，q_0 也是 5 的倍数.

$AB=OA+OB-2r=2r+p_0+q_0$.

由勾股定理，$AB^2=OA^2+OB^2$，即

$(2r+p_0+q_0)^2=(2r+p_0)^2+(2r+q_0)^2$，则

$p_0q_0=2r^2$，即

$p_0q_0=2\cdot 5^2\cdot 1994^2\cdot p^2$.

由$\frac{p_0}{5}$，$\frac{q_0}{5}$都是自然数，可得

$\frac{p_0}{5}\cdot\frac{q_0}{5}=2^3\times 977^2\times p^2$.

当 $p\neq 2$ 和 $p\neq 997$ 时，

$$\begin{cases}\dfrac{p_0}{5}=2^i\times 997^j\times p^k,\\[2mm]\dfrac{q_0}{5}=2^{3-i}\times 997^{2-j}\times p^{2-k}.\end{cases}$$

其中 $i=0,1,2,3$，$j=0,1,2$，$k=0,1,2$.

于是 $\left(\dfrac{p_0}{5},\dfrac{q_0}{5}\right)$ 有 $4\times3\times3=36$ 组不同的有序解.

当 $p=2$ 时，有

$$\begin{cases}\dfrac{p_0}{5}=2^i\times 997^j,\\[2mm]\dfrac{q_0}{5}=2^{5-i}\times 997^{2-j}.\end{cases}$$

其中 $i=0,1,2,3,4,5$，$j=0,1,2$.

于是 $\left(\dfrac{p_0}{5},\dfrac{q_0}{5}\right)$ 有 $6\times3=18$ 组不同的有序解.

当 $p=997$ 时，有

$$\begin{cases}\dfrac{p_0}{5}=2^i\times 997^j,\\[2mm]\dfrac{q_0}{5}=2^{3-i}\times 997^{4-j}.\end{cases}$$

这里 $i=0,1,2,3$，$j=0,1,2,3,4$.

于是 $\left(\dfrac{p_0}{5},\dfrac{q_0}{5}\right)$ 有 $4\times5=20$ 组不同的有序解.

由以上，所求直角三角形的个数：

$$S=\begin{cases}36, & \text{当 } p\neq2 \text{ 和 } p\neq997 \text{ 时},\\ 18, & \text{当 } p=2 \text{ 时},\\ 20, & \text{当 } p=997 \text{ 时}.\end{cases}$$

【解题思维策略分析】

1. 运用整数的性质求整点的数目

例 5 （1987 年全国高中数学联赛题）在坐标平面上，纵横坐标都是整数的点称为整点. 试证存在一个同心圆的集合，使得（1）每个整点都在此集合的某一圆周上；（2）此集合的每个圆周上，有且只有一个整点.

证法 1 假设同心圆圆心为 $P(x,y)$，任意两整点 $A(a,b)$ 和 $B(c,d)$，其中 $a=c$ 和 $b=d$ 不同时成立.

$|PA|^2=(x-a)^2+(y-b)^2=x^2+y^2-2ax-2by+a^2+b^2$,

$|PB|^2=(x-c)^2+(y-d)^2=x^2+y^2-2cx-2dy+c^2+d^2$,

$|PA|^2-|PB|^2=a^2-c^2+b^2-d^2+2(c-a)x+2(d-b)y$.

因为 $a,b,c,d\in\mathbf{Z}$，且 $a=c$，$b=d$ 不同时成立，

所以要使 $|PA|\neq|PB|$，只需取 x 为任意无理数，y 取任意分母不为 2 的非整数有理数即可(或 x,y 各取形如$\sqrt{m}$,$\sqrt{n}$的最简非同类根式的无理数，其中 $m,n\in\mathbf{N}$).

如取 $P\left(\sqrt{2},\frac{1}{3}\right)$，则任意两个不同整点到 $P\left(\sqrt{2},\frac{1}{3}\right)$的距离都不相等.

把所有整点到 P 的距离从小到大排成一列

r_1，r_2，r_3，…

以 $P\left(\sqrt{2},\frac{1}{3}\right)$为圆心，$r_1$，$r_2$，…，$r_n$，…为半径的同心圆集合即为所求.

证法 2 设任意两个不同整点 $A(a,b)$和 $B(c,d)$.

下面分三类情况进行讨论：

(i) $a\neq c$，$b\neq d$，中点 $M\left(\frac{a+c}{2},\frac{b+d}{2}\right)$.

AB 垂直平分线方程为

$$y-\frac{b+d}{2}=\frac{c-a}{b-d}\left(x-\frac{a+c}{2}\right).$$

(ii) $a=c$，$b\neq d$，中点 $M\left(a,\frac{b+d}{2}\right)$，$AB$ 垂直平分线方程为 $y=\frac{b+d}{2}$.

(iii) $a\neq c$，$b=d$，中点 $M\left(\frac{a+c}{2},b\right)$，$AB$ 垂直平分线方程为 $x=\frac{a+c}{2}$.

显然，只有在上述三类直线上的点才有可能到平面上某两整点的距离相等. 若取 $P(\sqrt{2},\sqrt{3})$，则 P 必然不在上述三类直线上，即 $P(\sqrt{2},\sqrt{3})$ 到任意两个不同整点的距离都不相等.

把所有整点与 P 点的距离从小到大排成一列：

r_1，r_2，r_3，…

以 $P(\sqrt{2},\sqrt{3})$ 为圆心，r_1，r_2，…，r_n，…为半径作的同心圆即为所求.

例 6 （1990 年全国高中数学联赛题）在坐标平面上，横坐标和纵坐标均为整数的点称为整点. 对任意自然数 n，连接原点 O 与点 $A_n(n,n+3)$，用 $f(n)$表示线段 OA_n 上除端点外的整点个数，求 $f(1)+f(2)+\cdots+f(1990)$的值.

解 易见，n 与$n+3$ 的最大公约数 $d=(n,n+3)$为

$$d=(n,n+3)=\begin{cases}3，当 3\mid n 时，\\ 1，当 3\nmid n 时.\end{cases}$$

首先证明 $d=(n,n+3)=1$ 时，线段 OA_n 内无整点.

否则，设 (m,l) 为 OA_n 内的一个整点，且满足 $1\leqslant m<n, 1\leqslant l<n+3$，则由

$\frac{m}{l}=\frac{n}{n+3}$，即 $m(n+3)=nl$，及 $(n,n+3)=1$ 可知

$n\mid m$，与 $m<n$ 矛盾.

当 $d=(n,n+3)=3$ 时，设 $n=3k$，则

线段 OA_n 内有两个整点 $(k,k+1),(2k,2k+2)$.

所以有 $f(k)=\begin{cases}2, 当\ 3\mid k\ 时,\\0, 当\ 3\nmid k\ 时.\end{cases}$

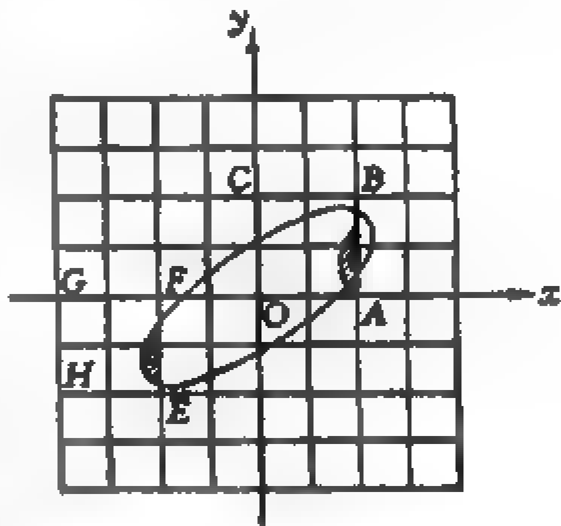
故 $f(1)+f(2)+\cdots+f(1990)=2\cdot\left[\frac{1990}{3}\right]=1326$.

2. 关注整点条件下的面积求解

例 7 （1979 年第 40 届美国普特南数学竞赛题）设 C 是平面上的闭凸集，C 除了包含（0，0）外，不包含其他坐标为整数的点，又设 C 分布在四个象限中的面积相等，证明 C 的面积 $A(C)\leqslant 4$.

证明 我们证明更为一般的结论：

如果一个关于原点对称的闭凸集，面积大于 4，那么，它的内部除原点外，一定还有别的整点.



如图，我们用分别和坐标轴距离是偶数的两组平行线，分平面成边长是 2 的较大的方格，其中标准的一个方格是 $OABC$，它是位于第一象限而离原点最近的一个方格，这些边长是 2 的方格把闭凸集分成许多块，每一个和这区域相交的较大方格中各有一块，例如图中 $EFGH$ 这个方格里就有一小块. 把 $EFGH$ 平移到 $OABC$，使两个方格重合，那么，$EFGH$ 里面所包含的一小块面积也就连带地被移到 $OABC$ 里面，如图中有阴影的那部分. 对于其他大方格中的面积可以用同样的方法移到正方形 $OABC$ 中去.

由于闭凸集的面积大于 4，而正方形 $OABC$ 的面积等于 4，所以由面积的重叠原则，至少有两块面积有公共点.

在移动每一个大方格时，可先沿 OX 轴的方向移动一段距离（等于 2 的倍数），再沿 OY 轴的方向移动一段距离（也等于 2 的倍数），最后就和 $OABC$ 重合. 因此，我们从两块面积移动后有公共点这个结论可推出，在原来的闭凸集内有两个点 P 和 Q，它们的纵坐标的差和横坐标的差都是 2 的倍数. 由对称性，P 关于原点的对称点 P' 也在这个闭凸集内.

设 P 的坐标为 (x_1,y_1)，则 P' 的坐标为 $(-x_1,-y_1)$，设 Q 的坐标是 (x_2,y_2)，那么 $P'Q$ 的中点 M 的坐标是 $\left(\frac{x_2-x_1}{2},\frac{y_2-y_1}{2}\right)$. 由于 x_2-x_1，y_2-y_1 是偶数，所以 $\frac{x_2-x_1}{2}$ 和 $\frac{y_2-y_1}{2}$ 一定是整数，因此 M 点一定是整点. 又由于 P 和 Q 是两个不同的点，则 $x_2-x_1\neq0$，$y_2-y_1\neq0$ 至少有一个成立，即 $M\left(\frac{x_2-x_1}{2},\frac{y_2-y_1}{2}\right)$ 不是原点 $(0,0)$，从而证明了题设中的闭凸集内除原点 $(0,0)$ 之外，至少还有一个整点.

例 8 （1986 年国家集训队选拔考试题）在平面直角坐标系中给定一个 100 边形 P，满足

(i) P 的顶点坐标都是整数；

(ii) P 的边都与坐标轴平行；

(iii) P 的边长都是奇数.

求证 P 的面积是奇数.

证法 1 先给出一个引理：

给定复平面上一个 n 边形 P，其顶点对应的复数分别为 $z_1,z_2,\cdots,z_n$，则 P 的有向面积为

$$S=\frac{1}{2}\mathrm{Im}(z_1\overline{z_2}+z_2\overline{z_3}+\cdots+z_{n-1}\overline{z_n}+z_n\overline{z_1}),$$

其中 $\mathrm{Im}(z)$ 表示复数 z 的虚部.

此引理可以利用 $n=3$ 时的结论，用数学归纳法加以证明.

下面证明命题本身.

设 P 的顶点对应的复数为

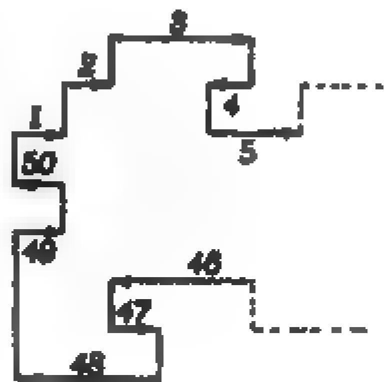
$z_j=x_j+iy_j$，$j=1,2,\cdots,100$.

由题设可知，x_j 和 y_j 都是整数.

再由题设 (ii) 和 (iii)，又可设

$$\begin{cases}x_{2j}=x_{2j-1},\\ y_{2j}=y_{2j-1}+\text{奇数},\end{cases}$$

$$\begin{cases}x_{2j+1}=x_{2j}+\text{奇数},\\ y_{2j+1}=y_{2j}.\end{cases}$$



这里 $1\leqslant j\leqslant50$，$x_{101}=x_1$，$y_{101}=y_1$，并约定 $y_0=y_{100}$.

由引理，P 的有向面积为

$$S=\frac{1}{2}\mathrm{Im}\sum_{j=1}^{100}z_j\overline{z_{j+1}}$$

$$=\frac{1}{2}\mathrm{Im}\sum_{j=1}^{100}(x_j+iy_j)(x_{j+1}-iy_{j+1})$$

$$=\frac{1}{2}\mathrm{Im}\sum_{j=1}^{100}[(x_jx_{j+1}+y_jy_{j+1})+i(x_{j+1}y_j-x_jy_{j+1})]$$

$$=\frac{1}{2}\sum_{j=1}^{100}(x_{j+1}y_j-x_jy_{j+1})$$

$$=\frac{1}{2}\sum_{j=1}^{50}(x_{2j+1}y_{2j}-x_{2j}y_{2j+1})+\frac{1}{2}\sum_{j=1}^{50}(x_{2j}y_{2j-1}-x_{2j-1}y_{2j})$$

$$=\frac{1}{2}\sum_{j=1}^{50}(x_{2j+1}y_{2j}-x_{2j-1}y_{2j})+\frac{1}{2}\sum_{j=1}^{50}(x_{2j-1}y_{2j-2}-x_{2j-1}y_{2j})$$

$$=\frac{1}{2}\sum_{j=1}^{50}(x_{2j+1}y_{2j}-x_{2j-1}y_{2j})+\frac{1}{2}\sum_{j=1}^{50}x_{2j+1}y_{2j}-\frac{1}{2}\sum_{j=1}^{50}x_{2j-1}y_{2j}$$

$$=\sum_{j=1}^{50}(x_{2j+1}y_{2j}-x_{2j-1}y_{2j})$$

$$=\sum_{j=1}^{50}(x_{2j+1}-x_{2j-1})y_{2j}$$

$$=\sum_{j=1}^{50}m_jy_{2j}\qquad(m_j\text{ 为奇数})$$

$$\equiv\sum_{j=1}^{50}y_{2j}\qquad(\mathrm{mod}\ 2)$$

$$\equiv\sum_{j=1}^{50}(y_{4j}-y_{4j-2})\qquad(\mathrm{mod}\ 2)$$

$$\equiv\sum_{j=1}^{25}1\qquad(\mathrm{mod}\ 2)$$

$$\equiv 1\qquad(\mathrm{mod}\ 2).$$

即 P 的面积是奇数.

证法 2 不妨设多边形 P 全在第一象限内（否则可经适当的平移化成这一情形）.

沿 P 的边界循顺时针方向绕行一周（P 始终在行进方向的右侧），依次将 50 条水平边编号为 1，2，…，50. 将底边在 OX 轴上，并且以第 i 号水平边为顶点的矩形条面积记为 S_i（$i=1$，2，…，50）.

于是，多边形 P 的面积可以表示成各 S_i 的代数和：

$$S=\sum_{i=1}^{50}(\pm S_i).$$

正负号则视沿该边前行时的方向与 OX 轴的方向相同或相反而定.

例如，图中多边形 P 的面积 S 表示为

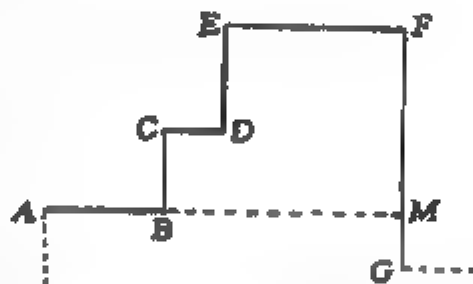
$S=S_1+S_2+S_3-S_4+S_5+\cdots-S_{46}+S_{47}-S_{48}+S_{49}-S_{50}$.

由于各矩形条的一条边长为奇数，则其面积的奇偶性由该矩形的高度决定.

由于边号相邻的两个矩形条，高度相差一个奇数，因而面积的奇偶性不同.

这样，在 50 个矩形条的面积当中，奇偶交替出现，从而恰有 25 个偶数和 25 个奇数，其代数和 S 必为奇数，即 100 边形 P 的面积是奇数.

证法 3 如图，设…$ABCDEFG$…为 100 边形的一部分.



延长 AB 交 FG 所在的直线于 M 点，易知 AM 的长和 GM 的长都是奇数，于是 96 边形…AMG…的各边长都是奇数.

容易求出，六边形 $BCDEFM$ 的面积为奇数，从而 100 边形和 96 边形的面积有不同的奇偶性，同理，96 边形和 92 边形有不同的奇偶性……，从而可推出 100 边形和 4 边形有相同的奇偶性，而边长都是奇数的满足条件的四边形的面积为奇数，于是所求的 100 边形的面积为奇数.

例 9 （1992 年全国高中数学联赛题）在平面直角坐标系中，横坐标和纵坐标都是整数的点称为整点，任取 6 个整点 $P_i(x_i,y_i)(i=1,2,3,4,5,6)$满足：

(1) $|x_i|\leqslant 2$，$|y_i|\leqslant 2(i=1,2,\cdots,6)$，

(2) 任何三点不在同一条直线上.

试证在以 $P_i(i=1,2,3,4,5,6)$ 为顶点的所有三角形中，必有一个三角形，它的面积不大于 2.

证法 1 设存在 6 个整点 P_1，P_2，…，P_6 落在区域 $S=\{(x,y)|\ |x|\leqslant 2,|y|\leqslant 2\}$内，它们任三个点所成的三角形面积都大于 2.

设 $P=\{P_1,P_2,\cdots,P_6\}$.

(1) 若 x 轴上只有 P 中的一个点，则剩下的 P 中的 5 个点，位于两个半平面，由抽屉原理在 x 轴的上半平面或下半平面一定有一个半平面上至少有三个点，不妨设 x 轴的上半平面至少有 P 的三个点，此三点所成的三角形面积不大于 2，因此，x 轴上至少有两个点. 又因为不能有三点共线，所以在 x 轴上恰有 P 的 2 个点.

(2) 剩下的 4 个点不可能有一点在直线 $y=\pm 1$ 上，否则出现 P 中的点为顶点的面积不大于 2 的三角形，于是在直线 $y=2$，$y=-2$ 上分别恰有 P 的两个点.

(3) 注意到 S 的对称性，同理可证在直线 $x=-2$，$x=0$，$x=2$ 上分别有 P 的两个点.

于是在每条直线 $y=-2$，0，2，$x=-2$，0，2 上恰有 P 的两个点.

(4) P 的点不能是原点. 这是因为 S 内纵横坐标均为偶数的所有整点落在且仅落在过原点的四条直线上, 由抽屉原理, 剩下的 5 个点至少有两点落在这些直线中的一条. 于是 3 点共线, 出现矛盾.

因此, P 在 x 轴上的两点必定是$(-2,0)$,$(2,0)$.

同理, 在 y 轴上的两点必定是$(0,-2)$,$(0,2)$.

剩下的两点只能取$(-2,-2)$, $(2,2)$或$(-2,2)$, $(2,-2)$, 不论哪一种情形, 都得到一个以 P 中的点为顶点的面积不大于 2 的三角形. 出现矛盾.

从而命题得证.

证法 2 设 P_i 中横坐标为 m 的点共有 a_m 个, 纵坐标为 n 的点共有 b_n 个$(m,n=-2, -1, 0, 1, 2)$.

由 P_i 满足的条件有

$0\leqslant a_m\leqslant 2$, $m=-2, -1, 0, 1, 2$,

$0\leqslant b_n\leqslant 2$, $n=-2, -1, 0, 1, 2$,

$a_{-2}+a_{-1}+a_0+a_1+a_2=6$,

$b_{-2}+b_{-1}+b_0+b_1+b_2=6$.

(1) 若 $a_m+a_{m+1}\geqslant 3$, 对某个 $m\in\{-2, -1, 0, 1, 2\}$ 成立, 则诸 P_i 中至少有 3 个点落在矩形区域 $\{m\leqslant x\leqslant m+1, -2\leqslant y\leqslant 2\}$ 的周界上, 此三点决定的三角形面积不大于 2.

(2) 若 $a_{-2}+a_{-1}\leqslant 2$, $a_{-1}+a_0\leqslant 2$, $a_0+a_1\leqslant 2$, $a_1+a_2\leqslant 2$, 由于

$$\begin{aligned}8&\geqslant(a_{-2}+a_{-1})+(a_{-1}+a_0)+(a_0+a_1)+(a_1+a_2)\\&=2(a_{-2}+a_{-1}+a_0+a_1+a_2)-(a_2+a_{-2})\\&=12-(a_2+a_{-2}),\end{aligned}$$

于是 $a_2+a_{-2}\geqslant 4$.

再由没有三点共线, 所以

$a_2=2$, $a_{-2}=2$, $a_1=0$, $a_{-1}=0$, $a_0=2$.

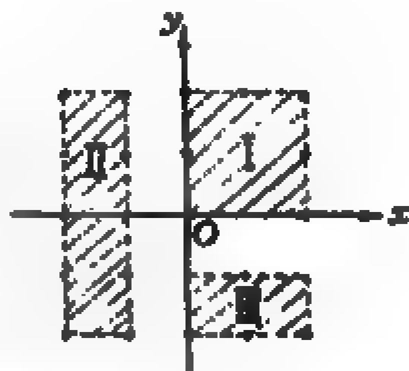
即在直线 $x=2i$ $(i=0, \pm1)$ 上恰有 P 的两个点, 同理可证直线 $y=2i$ $(i=0, \pm1)$ 上恰有 P 的两个点.

以下同证法 1.

证法 3 设存在满足条件的 6 个整点 P_1, P_2, …, P_6 落在区域$\{(x,y)\mid |x|\leqslant 2, |y|\leqslant 2\}$内, 任何 3 个点所组成的三角形面积都大于 2.

把 25 个整点(m,n), $m,n\in\{-2,-1,0,1,2\}$, 分成如图的三个组, 第Ⅰ组为$\{(m,n)\mid m=0,1,2,n=0,1,2\}$, 共 9 个点, 面积为 4; 第Ⅱ组为$\{(m,n)\mid m=-1,-2,n=-2,-1,0,1,2\}$共 10 个点, 面积为 4; 第Ⅲ组为$\{(m,n)\mid m=0,1,2,n=-2,-1\}$, 共 6

个点.



为使三角形的面积大于 2，则落入第Ⅰ组内的点不超过 2 个，落入第Ⅱ组内的点不超过 2 个，否则将出现一个以 P_i 为顶点的面积不大于 2 的三角形，因此，至少有两点落在第Ⅲ组内，记第Ⅲ组为

$D_4=\{(x,y)|0\leqslant x\leqslant 2,-2\leqslant y\leqslant -1\}$.

同理，对这 25 个点重新划分区域，使上述的第Ⅲ组分别落在第Ⅰ、Ⅱ、Ⅲ象限内，则

$D_1=\{(x,y)|0\leqslant y\leqslant 2,1\leqslant x\leqslant 2\}$,

$D_2=\{(x,y)|-2\leqslant x\leqslant 0,1\leqslant y\leqslant 2\}$,

$D_3=\{(x,y)|-2\leqslant x\leqslant -1,-2\leqslant y\leqslant 0\}$.

从而 D_1，D_2，D_3，D_4 覆盖了除（0，0）之外的已知点中的 24 个整点，且每个区域的边界上至少有两个点，由于这四个区域互不相交，所以总共有 8 个点，与已知的 6 个点矛盾！

3. 关注整点条件下的各类问题求解

例 10 （1986 年全国高中数学联赛题）平面直角坐标系中，纵、横坐标都是整数的点称为整点. 请设计一种方法将所有的整点染色，每点染成白色、红色或黑色中的一种颜色，使得：(1) 每一种颜色的点，出现在无穷多条平行于横轴的直线上；(2) 对任意的白点 A，红点 B 和黑点 C，总可以找到一个红点 D，使得 $ABCD$ 是一平行四边形. 证明你设计的方法符合上述要求.

解 设计如下的染色方法：把（奇、奇）类格点染成白色，（偶，偶）类格点染成黑色，（奇，偶）和（偶，奇）类格点染成红色，易知这种染色方法满足条件(1).

任取白点 $A(2m+1,2n+1)$，黑点 $C(2s,2t)$，红点 $B(2p,2q+1)$，其中 m，n，s，t，p，q 均为整数，再设平行四边形 $ABCD$ 的顶点 D 的坐标为 (x,y).

由平行四边形对角线互相平分及中点坐标公式得

$$\begin{cases}x+2p=2m+1+2s,\\ y+2q+1=2n+1+2t,\end{cases}$$

解出 $x=2m+1+2s-2p$，$y=2(n+t-q)$.

由此可得 $D(x,y)$ 是（奇，偶）类格点，所染的色也是红色.

同理，若点 B 是（奇，偶）类格点，可推得 D 是（偶，奇）类格点，所染的色也是红色，故这样的设计方案也满足 (2).

例 11 （1986 年第 49 届莫斯科数学奥林匹克题）以平面直角坐标系中的每一

个整点为圆心，各作一个半径为$\frac{1}{14}$的圆．证明任何半径为100的圆周都至少与这些圆中的一个相交．

证明 设O为任意一个点．

又设$y=k$（$k\in\mathbf{Z}$）是与以O为圆心、以100为半径的圆相交的直线中最上面的一条直线，而直线$y=k+1$与该圆不相交．

如果该直线上所有的整点都在该圆之外，那么不难证明，其中离圆周最近的整点与圆周的距离不超过$\frac{1}{14}$，因此圆周必与以该整点为圆心、以$\frac{1}{14}$为半径的圆相交．

如果该直线$y=k$上有某些整点在该圆O之内，设B是其中离该圆周最近的整点，设A是直线$y=k$上离B最近的位于圆外的整点，则有$AB=1$．

假设圆周不与以A和B为圆心、以$\frac{1}{14}$为半径的圆相交，则此时就有

$$OA>100+\frac{1}{14},\quad 99<OB<100-\frac{1}{14},$$

因此就有

$$OA-OB>\frac{1}{7},$$

$$OA^2-OB^2=(OA-OB)(OA+OB)>\frac{199}{7}.$$

设O'是自O向直线$y=k$所引垂线之垂足，$O'B=x$，则

$$O'A=x+1,$$

$$(x+1)^2-x^2=OA^2-OB^2>\frac{199}{7},$$

解得 $O'B=x>\frac{96}{7}$．

于是就有

$$OO'=OB^2-O'B^2<\left(100-\frac{1}{14}\right)^2-\left(\frac{96}{7}\right)^2<99^2,$$

从而$OO'<99$．

由于圆心O到直线$y=k+1$的距离为

$$OO'+1<99+1=100,$$

这样该圆就与直线$y=k+1$相交，与我们一开始的选取相矛盾．

因此该圆必与圆A或圆B之一相交．

例12 （*第44届斯洛文尼亚国家队选拔赛题*）给定一个$N\times N$的网格，从第一个格点（1，1）出发，按以下规则进行移动：

(1) 由格点 (a, b) 可以移到格点 $(2a, b)$ 或 $(a, 2b)$;

(2) 由格点 (a, b) 可以移到格点 $(a-b, b)$，其中 $a>b$;

(3) 由格点 (a, b) 可以移到格点 $(a, b-a)$，其中 $b>a$.

问：对哪些正整数 x，y，可以移动到对应的格 (x, y) 上?

解 设 $d(x,y)$ 为 x，y 的最大奇公约数. 易知，按题设规则从 (a,b) 移到 (e,f) 时，有

$$d(a,b)=d(e,f).$$

因为 $d(1,1)=1$，故当 $d(x,y)>1$ 时，不可能从 $(1,1)$ 移到 (x,y).

当 $d(x,y)=1$ 时，不妨设 x,y 全为奇数.

作如下的逆移动：

若 $x>y>1$，$x+y=2^k x_1$，其中 x_1 为奇数，则

$$(x,y)\leftarrow(x+y,y)\leftarrow\left(\frac{x+y}{2^k}=x_1,y\right);$$

若 $x_1>y$，继续作逆移动，得到一串奇数列

$$x>x_1>x_2>\cdots>x_{n-1}\ (>y).$$

由 $d(x,y)=1\neq y$，必存在 $x'<y$，使得

$$(x,y)\leftarrow(x',y).$$

继续作如上的逆移动，得到一串奇数列：

$$x>y>x'>y'>\cdots>1=1.$$

即得到逆移动：

$$(x,y)\leftarrow(x',y)\leftarrow(x',y')\leftarrow\cdots\leftarrow(1,1).$$

故当 $d(x,y)=1$ 时，可以从 $(1,1)$ 移到 (x,y).

例 13 （2004 年克罗地亚数学竞赛题）一只青蛙在平面直角坐标系上从点 (1, 1) 开始按照如下规则跳跃：(1) 该青蛙能从任一点 (a, b) 跳到点 $(2a, 6)$ 或 $(a, 2b)$；(2) 如果 $a>b$，该青蛙能从 (a, b) 跳到 $(a-b, b)$，如果 $a<b$，该青蛙能从 (a, b) 跳到 $(a, b-a)$.

问：这只青蛙能到达点①(24,40)，②(40,60)，③(24,60)，④(200,4)吗?

解 对①，④，答案是肯定的. 我们给出青蛙从点(1,1)到给定点的路径实例：

①的路径是

$(1,1)\to(2,1)\to(4,1)\to(3,1)\to(3,2)\to(3,4)\to(3,8)\to(3,5)\to(6,5)\to(12,5)\to(24,5)\to(24,10)\to(24,20)\to(24,40)$.

④的路径是

$(1,1)\to(2,1)\to(4,1)\to(8,1)\to(16,1)\to\cdots\to(64,1)\to(63,1)\to(62,1)\to(61,1)\to(60,1)\to\cdots\to(50,1)\to(50,2)\to(50,4)\to(100,4)\to(200,4)$.

对于②,③,答案是否定的,用规则(1)和规则(2)都不能到达 x 和 y 有公共奇因子(大于 1)的点(x,y). 而 40 和 60 都能被 5 整除,24 和 60 都能被 3 整除,因此,青蛙从点(1,1)出发不能到达(40,60)和(24,60).

4. 借助于整点处理问题

例 14 (1971 年第 32 届美国普特南数学竞赛题)某人掷硬币,得正面记 a 分,得背面记 b 分(a,b 为正整数,$a>b$),并将每次得分进行累计. 他发现不论掷多少次,总有 35 个分数记录不到,例如 58 就是其中之一. 试确定 a 和 b 的大小.

解 设某人掷硬币得正面 x 次,得背面 y 次,其中 x 和 y 均为非负整数.

于是累计得分 $ax+by$ 分.

首先证明$(a,b)=1$.

否则,若$(a,b)=d>1$,那么 $ax+by$ 恒能被 d 整除,这样,与 d 互素的一切正整数(如 $kd+1$)都是无法达到的分数,于是有无限多个无法达到的分数,与已知条件矛盾.

因此$(a,b)=1$.

显然,如果 m 是可以达到的一个分数,那么直线 $ax+by=m$ 至少通过包括横轴、纵轴的正半轴和原点在内的第一象限(即闭的第一象限)的整点.

因为$(a,b)=1$,所以

$b\cdot 0,b\cdot 1,\cdots,b\cdot(a-1)$这 a 个数被 a 除的余数互不相同.

这是因为若 $bi\equiv bj\pmod a$,则由$(a,b)=1$ 得 $i-j\equiv 0\pmod a$.

而$|i-j|<a$,所以是不可能的.

因此,当 $m\geqslant ab$ 时,$m-b\cdot 0$,$m-b\cdot 1$,$\cdots$,$m-b(a-1)$ 中恰有一个能被 a 整除,即存在 $y(0\leqslant y\leqslant a-1)$及非负整数 x,使

$m-by=ax$.

所以 $m\geqslant ab$ 时,m 必是可以达到的分数,然而,由题意,可达到的分数只有有限个,所以 $m\geqslant ab$ 不成立.

当 $0\leqslant m<ab$ 时,若 m 是可以达到的分数,那么直线 $ax+by=m$ 只含闭的第一象限的一个整点.

若不然,设(x_1,y_1),(x_2,y_2)都在直线 $ax+by=m$ 上,则

$ax_1+by_1=m$,$ax_2+by_2=m$,

于是有 $a(x_1-x_2)+b(y_1-y_2)=0$,

从而 $b\mid x_1-x_2$.

但是 $0\leqslant ax_1\leqslant m<ab$,所以

$0\leqslant x_1<b$.

同理 $0\leqslant x_2<b$.

即 $|x_1-x_2|<b$.

于是仅当 $x_1=x_2$ 时，才有 $b\mid x_1-x_2$，出现矛盾.

于是 $0\leqslant m<ab$ 时，所能达到的分数的个数与闭的第一象限中，使 $0\leqslant ax+by<ab$ 的整点 (x,y) 的个数相同.

注意到，矩形 $0\leqslant x\leqslant b$，$0\leqslant y\leqslant a$ 中，有 $(a+1)(b+1)$ 个整点，所以在闭的第一象限中，使 $0\leqslant ax+by<ab$ 的整点 (x,y) 的数目是 $\frac{1}{2}(a+1)(b+1)-1$.

所以，不可能达到的分数的个数是

$$ab-\left[\frac{1}{2}(a+1)(b+1)-1\right]=\frac{1}{2}(a-1)(b-1).$$

依题意有

$$\frac{1}{2}(a-1)(b-1)=35.$$

因为 $a>b$，且 $(a,b)=1$，则有

$$\begin{cases}a-1=70,\\ b-1=1\end{cases} \text{或} \begin{cases}a-1=10,\\ b-1=7\end{cases} \text{或} \begin{cases}a-1=35,\\ b-1=2.\end{cases}$$

即 $(a,b)=(71,2),(11,8),(36,3)$.

由 $(a,b)=1$，则 $(36,3)$ 不可能.

又 $a=71$，$b=2$ 时，

$$71\cdot 0+2\cdot 29=58$$

能被记录到，所以 $a=71$，$b=2$ 不合题意.

再考察直线 $11x+8y=58$ 上的整点，由

$$y=\frac{58-11x}{8}=7-x+\frac{2-3x}{8}$$

可以求得直线上的两个相邻整点 $(6,-1)$ 及 $(-2,10)$ 分别位于第四、第二象限，因此 58 不能被记录到. 从而 $a=11$，$b=8$ 是适合本题要求的唯一解.

例 15 （2005 年巴尔干地区数学奥林匹克题）在一个 2004×2004 的棋盘上放置了 2004 个女王，使其中任何两个女王都不能互相攻击（即不在同一行、同一列和同一条斜线上）. 证明：存在两个女王，使她们的外接矩形（即两个女王位于矩形对角线的两端）的半周长等于 2004.（假定每个女王都恰好位于她所占据的方格的中心.）

证明 用 1，2，…，2004 分别表示方格中心所对应的行与方格中心所对应的列，于是，可假定每个女王的坐标为 $(i,a_i)(i=1,2,\cdots,2004)$，而 a_1，a_2，…，a_n 是 1，2，…，2004 的一个排列.

由于两个不同的女王不能位于同一条斜线上，因此，当 $i\neq j$ 时，一定有

$\frac{a_i-a_j}{i-j}\neq 1.$ ①

于是，所证的结论可表述为：存在着 1，2，…，2004 中的一个数对(i,j)，满足 $|i-j|+|a_i-a_j|=2004$.

为了证明这一点，对任何 i，令 $x_i=a_i-i$.

显然，$\sum_{i=1}^{n}x_i=0$，且 $|x_i|<2004$.

由式①可知，当 $i\neq j$ 时，$x_i\neq x_j$.

下面证明：存在 i，j，使 $x_i-x_j=2004$.

用反证法证明.

否则，数 x_1，x_2，…，x_{2004} 关于模 2004 将得到不同的余数，这时，一定有

$$\sum_{i=1}^{n}x_i\equiv 1+2+\cdots+2004=1002\times 2005\not\equiv 0 \pmod{2004}.$$ 矛盾.

于是，一定存在 i，j，使 $x_i-x_j=2004$，即

$a_i-a_j+j-i=2004.$

易知 $|a_i-a_j|<2004$，$|j-i|<2004$，则

$a_i-a_j>0$，$j-i>0$.

故 $|i-j|+|a_i-a_j|=a_i-a_j+j-i=2004.$

【模拟实战】

1. （1984 年北京市数学竞赛题）证明曲线 $y=\frac{1}{5}(x^2-x+1)$ 不可能经过两个坐标都是整数的点.
2. 在平面上考虑由整点构成的点网络，试对具有有理斜率的直线证明下述结论：
   (1) 这样的直线或者不通过网络点，或者通过无穷多个网络点.
   (2) 对于每一条这样的直线，都存在一个正数 d，使得除去直线上可能有的网络点之外，再没有网络点与直线的距离小于 d.
3. （1977 年第 40 届莫斯科数学奥林匹克题）将数轴上每一个坐标为整数的点或染为红色，或染为蓝色. 证明至少有一种颜色具有下述性质：即对每个自然数 k，都能找到无穷多个染了这种颜色的点，它们的坐标都能被 k 整除.
4. （1988 年第 14 届全俄数学奥林匹克题）方格纸上小方格的尺寸为 1×1，以其中的一个结点（方格线的交点）为圆心画一个半径为 R 的圆周. 试证，如果在圆周上刚好有 1988 个结点，则 R 和 $\sqrt{2}R$ 中有一个是整数.
5. （1979 年四川省数学竞赛题）设 x，y 是使 $xy-1$ 能被素数 1979 除尽的整数，以

(x,y) 为坐标的那些点，如果有三点在一条直线上，求证这三点中至少有两点，它们的横坐标之差与纵坐标之差都能被 1979 除尽.

6. (IMO－30 预选题) R 为一个长方形，它是若干个长方形 $\{R_i \mid 1\leqslant i\leqslant n\}$ 的并集，满足

(1) R_i 的边与 R 的边平行；

(2) R_i 互不重叠；

(3) 每个 R_i 都至少有一条边长为整数.

证明 R 至少有一条边长是整数.

7. (第 54 届白俄罗斯数学奥林匹克题) 在 $n\times n(n\geqslant 3)$ 的方格表的每个格中填入一个确定的整数. 已知任意 3×3 的单元中所有数之和为偶数，同时，任意 5×5 的单元中所有数之和也为偶数. 求使得此方格表中所有之和为偶数的全部 n.

8. 空间中有一凸多面体，它的所有顶点都是整点（每个顶点的三个坐标值都是整数），此外，在多面体的内部、面上和棱上都不再有其他整点，问这个凸多面体顶点个数的最大值是多少.

9. (第 31 届俄罗斯数学奥林匹克题) 在方格纸上画一个矩形，它的边与方格交成 45° 的角，它的顶点都不在方格线上. 试问：矩形的各条边能否都刚好穿过奇数条方格线?

参考解答

第一章 整数的离散性与封闭性运算

1. (1) 假设 n 有 $k+1$ 位数，$k\in\mathbf{N}$，则

$n=10^k a_k+10^{k-1}a_{k-1}+\cdots+10a_1+a_0$，其中，$a_1$，$a_2$，…，$a_k\in\{1,2,\cdots,9\}$.

于是，有 $p(n)=a_0a_1\cdots a_k\leqslant a_k9^k\leqslant a_k10^k\leqslant n$.

因此，$p(n)\leqslant n$.

(2) 首先，由 $n^2+4n-2005\geqslant0$，得 $n\geqslant43$.

其次，由 $n^2+4n-2005=10p(n)\leqslant10n$，得 $n\leqslant47$.

从而，推断出 $n\in\{43,44,45,46,47\}$.

逐一检验知 $n=45$.

2. 将方程 $\sqrt{x}=\sqrt{2004}-\sqrt{y}$ 两边平方，整理得

$2\sqrt{2004y}=2004+y-x$.

由此可知 $2\sqrt{2004y}=4\sqrt{501y}$ 是个整数. 于是，$y=501k^2$，其中 k 是非负整数（由于 $501=3\times167$，因此设 $y=501k^2$ 是合理的）.

将 y 的表达式代入原方程，可得

$\sqrt{x}=(2-k)\sqrt{501}$，由此可得出 k 为 0，1，2.

所以，所有可能的数对 (x,y) 为 $(2004,0)$，$(501,501)$，$(0,2004)$.

3. 设立方体的每个面上的数字分别为 a_1，a_2，a_3，a_4，a_5，a_6，在顶点上所写的数分别为

$a_1a_2a_5$，$a_2a_3a_5$，$a_3a_4a_5$，$a_4a_1a_5$，$a_1a_2a_6$，$a_2a_3a_6$，$a_3a_4a_6$，$a_4a_1a_6$.

于是，可得

$$\begin{aligned}70&=a_1a_2a_5+a_2a_3a_5+a_3a_4a_5+a_4a_1a_5+a_1a_2a_6+a_2a_3a_6+a_3a_4a_6+a_4a_1a_6\\&=(a_5+a_6)(a_1a_2+a_2a_3+a_3a_4+a_4a_1)\\&=(a_1+a_3)(a_2+a_4)(a_5+a_6).\end{aligned}$$

由于 $70=2\times5\times7$，显然，在乘积

$(a_1+a_3)(a_2+a_4)(a_5+a_6)$

中，一个因子等于 2，一个因子等于 5，另一个因子等于 7.

于是，所求的和为

$a_1+a_2+a_3+a_4+a_5+a_6=2+5+7=14$.

4. 假定已得到了 n 个连续整数之和，其中最大数为 m，显然 $m>0$. 由于这个和等于正数 n，

可得

$$n=m+(m-1)+\cdots+[m-(n-1)]=nm-[1+2+\cdots+(n-1)]=nm-\frac{1}{2}(n-1)n.$$

最后一式可化简为 $1=m-\frac{1}{2}(n-1)$.

因此，n 一定是个奇数，对任何一个正奇数 n，序列中的最大整数 $m=1+\frac{n-1}{2}=\frac{n+1}{2}$. 这 n 个连续的整数和，可以这样写出：

以 $-\frac{n-3}{2}$ 开始，以 $\frac{n+1}{2}$ 结束，这个和恰好等于 n.

5. 由定义可知 a_n 是正数. 由于

$a_{n+3}a_n=a_{n+1}a_{n+2}+7$，

$a_{n+4}a_{n+1}=a_{n+2}a_{n+3}+7$，

两式相减得

$a_{n+3}a_n-a_{n+4}a_{n+1}=a_{n+1}a_{n+2}-a_{n+2}a_{n+3}$.

所以，$\frac{a_n+a_{n+2}}{a_{n+1}}=\frac{a_{n+2}+a_{n+4}}{a_{n+3}}$.

令 $b_n=\frac{a_n+a_{n+2}}{a_{n+1}}$，则 $b_{n+2}=b_n$.

由于 $a_1=9$，易得 $b_1=3$，$b_2=5$，即

$b_{2k-1}=\frac{a_{2k-1}+a_{2k+1}}{a_{2k}}=3$，

$b_{2k}=\frac{a_{2k}+a_{2k+2}}{a_{2k+1}}=5$.

于是，$a_{2k+1}=3a_{2k}-a_{2k-1}$，

$a_{2k+2}=5a_{2k+1}-a_{2k}$.

从而，有

$a_{2k+3}=13a_{2k+1}-a_{2k-1}$，

$a_{2k+2}=13a_{2k}-a_{2k-2}$.

对于任意的正整数 n，有

$a_{n+4}=13a_{n+2}-a_n$.

所以，a_n 均为整数.

6. 易知，正整数的平方是两位的有：16，25，36，49，64，81.

注意到，从给出数字开始至多有 1 个两位平方，因此，在第 1 个两位数被选定后，所求数的余下部分被唯一地确定. 因为没有以 5 或 9 开始的两位的平方数，所以，所求的数不能以 25 或 49 开始.

而由 16 得 164，1649；

由 36 得 364，3649；

由 64 得 649；

由 81 得 816，8164，81649.

因此，满足条件的数为

164，1649，364，3649，649，816，8164，81649.

7. 如果(x,y) 是给定方程组的一组整数解，将两个式子相减，得到

$x^2-y^2=y-x \Leftrightarrow (x-y)(x+y+1)=0$.

考虑下列两种情况.

(1) $x-y=0$.

将 $x=y=m$ 代入方程组得

$a=m^2-m=m(m-1)$.

易知 a 是两个连续整数的积.

故 a 是非负的，这些数不大于 2005.

又 $45\times 44=1980<2005$，

$46\times 45=2070>2005$，

因为 m 可以取 $1\leqslant m\leqslant 45$ 中的所有整数，这样，就有 45 个 a 满足条件.

(2) $x+y+1=0$.

将 $x=m$，$y=-(m+1)$ 代入方程组得

$a=m^2+m+1=m(m+1)+1$.

易知 a 比两个连续整数的积大 1. 由第一种情况中得到的 a 加上 1 就得到第二种情况中的 a，也有 45 个不同的 a 满足条件.

综上所述，总共有 90 个 a 满足条件.

8. 显然，$1\in B$ [否则，$1\in A$，由条件 (3)，对任意的 $b\in B$，有 $1\times b=b\in A$，矛盾].

对任意的 $a\in A$，由条件 (2)，$a+1\in B$，从而，对任意的 $k\in\mathbf{N}$，$ka+1\in B$.

故 $2\in B$ [否则，$2\in A$，知对任意的 $k\in\mathbf{N}$，$2k+1\in B$，有 $13\in B$，矛盾].

同理，3，4，6，$12\in B$，即对任意的 $a\in A$，$a-1$ 的任一因子属于 B.

由条件 (3)，对任意的 $a\in A$，有 $2a$，$3a\in A$.

由 $13\in A$，有 $13+1=14\in B$，故 $7\in B$ [否则，$7\in A$，有 $14\in A$，矛盾]；

由 $2\times 13+1=27\in B$，有 $9\in B$；

由 $3\times 13+1=40\in B$，有 20，10，$5\in B$，且 $8\in B$ [否则，$8\in A$，有 $8\times 5=40\in A$，矛盾]；

由 $5\times 13+1=66\in B$，有 33，22，$11\in B$.

综上，$\{1,2,\cdots,12\}\subseteq B$，$13\in A$.

由条件 (2)，对任意的 $k\in\mathbf{N}$，$i=1$，2，…，12，有 $13k+i\in B$.

由条件 (3)，对任意的 $k\in\mathbf{N}$，$i=1$，2，…，12，有 $13(13k+i)\in A$. 特别地，$13i\in A(i=1,2,\cdots,12)$.

若 $13^2t\in B$ $(t\in\mathbf{N}_+)$，则由条件 (2)，有

$13^2t+13i=13(13t+i)\in B$，矛盾.

故对任意的 $t\in\mathbf{N}_+$，$13^2t\in A$.

所以，$A=\left\{13t \mid t=1,2,\cdots,\left[\frac{2006}{13}\right]\right\}$，$B=S-A$. 经检验，满足条件.

故$|A|=\left[\frac{2006}{13}\right]=154$.

9. 显然 $f(n)=n$ 满足条件.

令 $m=n=0$，有 $f(0)=2[f(0)]^2$，则

$f(0)=0$ 或$\frac{1}{2}$，但$\frac{1}{2}$不是整数，所以，

$f(0)=0$.

令 $m=0$，$n=1$，有

$f(1)=[f(0)]^2+[f(1)]^2$，即 $f(1)=[f(1)]^2$.

则 $f(1)=0$ 或 1，但 $f(1)>0$，所以，$f(1)=1$.

设 $S=\{n \mid n\in \mathbf{N}$，且 $f(n)=n\}$，则 1，$0\in S$.

首先证明 S 的三条性质.

(i) 若 a，$b\in S$，则 $a^2+b^2\in S$.

证明：因为 a，$b\in S$，则 $f(a)=a$，$f(b)=b$，故

$f(a^2+b^2)=[f(a)]^2+[f(b)]^2=a^2+b^2$.

所以，$a^2+b^2\in S$.

(ii) 若 $a\in S$，$a^2+b^2\in S$，则 $b\in S$.

证明：因为 $a\in S$，$a^2+b^2\in S$，则

$f(a)=a$，

$f(a^2+b^2)=a^2+b^2$.

而 $f(a^2+b^2)=[f(a)]^2+[f(b)]^2$，所以，

$a^2+b^2=a^2+[f(b)]^2$.

从而，$[f(b)]^2=b^2$，即 $f(b)=b$.

故 $b\in S$.

(iii) 若 $a^2+b^2=c^2+d^2$，且 b，c，$d\in S$，则 $a\in S$.

证明：因为 c，$d\in S$，由 (i) 有 $c^2+d^2\in S$.

所以，$a^2+b^2\in S$.

再由 $b\in S$ 及 (ii) 知 $a\in S$.

其次是从 0，$1\in S$ 推出 0，1，2，…，$15\in S$.

$2=1^2+1^2$，由 (i)，$2\in S$.

$5=1^2+2^2$，由 (i)，$5\in S$.

$4=0^2+2^2$，由 (i)，$4\in S$.

$3^2+4^2=5^2+0^2$，由 (iii)，$3\in S$.

$7^2+1^2=5^2+5^2$，由 (iii)，$7\in S$.

$8=2^2+2^2$，由 (i)，$8\in S$.

$9=3^2+0^2$，由 (i)，$9\in S$.

$10=3^2+1^2$，由(i)，$10\in S$.

$6^2+8^2=10^2+0^2$，由(iii)，$6\in S$.

$11^2+2^2=10^2+5^2$，由(ii)，$11\in S$.

$13=2^2+3^2$，由(i)，$13\in S$.

$12^2+5^2=13^2+0^2$，由(iii)，$12\in S$.

$14^2+2^2=10^2+10^2$，由(iii)，$14\in S$.

$15^2+0^2=12^2+9^2$，由(iii)，$15\in S$.

最后证明 $S=\mathbf{N}$.

用数学归纳法.

假设 $1, 2, \cdots, 8k-2, 8k-1, 0\in S$，由

$(8k)^2+k^2=(7k)^2+(4k)^2$,

$(8k+1)^2+(k-3)^2=(7k-1)^2+(4k+3)^2$,

$(8k+2)^2+(k-1)^2=(7k+1)^2+(4k+2)^2$,

$(8k+3)^2+(k+1)^2=(7k+3)^2+(4k+1)^2$,

$(8k+4)^2+(k+3)^2=(7k+5)^2+(4k)^2$,

$(8k+5)^2+k^2=(7k+4)^2+(4k+3)^2$,

$(8k+6)^2+(k+2)^2=(7k+6)^2+(4k+2)^2$,

$(8k+7)^2+(k+4)^2=(7k+8)^2+(4k+1)^2$,

及(iii)知 $8k, 8k+1, \cdots, 8k+7\in S$，这里 $k\geqslant 2$.

而已有 $1, 2, \cdots, 15, 0\in S$，则 $S=\mathbf{N}$.

故对所有非负整数 n，$f(n)=n$.

10. 容易验证 $S=\{-1,0,1\}$ 满足条件.

下面证明：$|S|_{\max}=3$.

(1) $1, -1$ 中至少有一个属于 S.

反之，存在 $a_1, a_2\in S$，且

$|a_1|, |a_2|\geqslant 2(|a_2|\geqslant|a_1|)$.

由题意，存在 $a, b, c\in S$，对于 a_1, a_2 满足题设.

故 $\frac{c}{a}=a_1a_2\Rightarrow c=aa_1a_2$.

则存在 $a_3=c\in S$，且

$|a_3|=|a||a_1||a_2|>|a_2|\geqslant|a_1|$.

重复上述过程得 $a_i(i=1,2,\cdots)\in S$，且 $|a_1|\leqslant|a_2|<|a_3|<\cdots<|a_i|<\cdots$，与 S 是有限集矛盾.

(2) 不妨设 $1\in S$，存在 $a_1\in S(a\neq 1)$.

则由题意，存在 $a, b, c\in S$，使得

$$\begin{cases}a+b+c=0\Rightarrow b=-a-c,\\ a_1+1=-\frac{b}{a}=1+\frac{c}{a}.\end{cases}$$

故 $a_1=\frac{c}{a}\Rightarrow c=aa_1$.

(i) $a_1\geqslant 2$.

若 $a\neq\pm 1$，则 $|c|>|a_1|$. 存在 $a_2=c\in S(|a_2|>|a_1|)$.

故存在 $|a_1|<|a_2|<\cdots\in S$.

矛盾.

若 $a=1$，$b=-a_1-1$；$a=-1$，$b=a_1+1$.

则无论 $a=\pm 1$，均有 $|b|>|a_1|$. 同上也推出矛盾.

(ii) $a_1\leqslant -2$.

考虑 $-\frac{b}{a}=a_1+1$，$\frac{c}{a}=a_1$.

由假设不存在 $a\in S$，且 $a\geqslant 2$.

因 $a_1\leqslant -2$，$b=-a(a_1+1)$，$c=aa_1$，所以，b 与 c 异号.

当 $a\leqslant -2$ 时，$c>|a_1|\geqslant 2$. 矛盾.

当 $a=-1$ 时，$b=a_1+1$，$c=-a_1\geqslant 2$. 矛盾.

当 $a=1$ 时，$b=-a_1-1$，$c=a_1$.

若当 $a_1\leqslant -3$ 时，$b\geqslant 2$. 矛盾.

由 (i)、(ii) 知，$a_1\in\{-2,-1,0\}$.

显见，$S=\{-2,-1,0,1\}$ 不满足条件.

事实上，对 -1、$-2\in S$，$x^2+3x+2=0$，不可能.

从而，$|S|_{\max}=3$.

11. 由于 $\{1,2,\cdots,n\}$ 可分拆成若干个三元数组，则 $3|n$.

又因每个三元数组均可表示成 $\{a,b,a+b\}$ 的形式，所以，每个三元数组的元素之和为偶数.

因此，$\{1,2,\cdots,n\}$ 的元素之和为偶数，即 $4|n(n+1)$.

综上，n 必为 $12k$ 或 $12k+3$ 的形式.

因此，$n=3900$ 或 $n=3903$.

最后证明：当 $n=3900$ 或 $=3903$ 时，均存在满足题意的分拆.

引理　假设当 $n=k$ 时，存在满足题意的分拆，则当 $n=4k$ 或 $n=4k+3$ 时，也存在满足题意的分拆.

引理的证明：由于集合 $\{1,2,\cdots,k\}$ 满足分拆条件，故可对集合 $\{2,4,\cdots,2k\}$ 以同样方式进行分拆.

对于 $n=4k$ 还剩下数

$\{1,3,\cdots,2k-1,2k+1,2k+2,\cdots,4k-1,4k\}$.

可将其分拆成 k 个三元数组

$\{2j-1,3k-j+1,3k+j\}(j=1,2,\cdots,k)$.

如下每列为一个三元数组：

$$\begin{pmatrix} 1 & 3 & 5 & \cdots & 2k-3 & 2k-1 \\ 3k & 3k-1 & 3k-2 & \cdots & 2k+2 & 2k+1 \\ 3k+1 & 3k+2 & 3k+3 & \cdots & 4k-1 & 4k \end{pmatrix}.$$

对于 $n=4k+3$，还剩下数

$\{1,3,\cdots,2k-1,2k+1,\cdots,4k+2,4k+3\}$.

可将其分拆成 $k+1$ 个三元数组

$\{2j-1,3k+3-j,3k+j+2\}(j=1,2,\cdots,k+1)$.

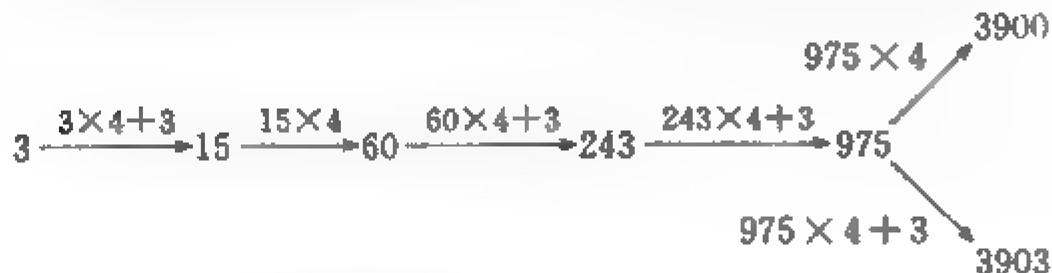
同样得到如下每列为一个三元数组：

$$\begin{pmatrix} 1 & 3 & 5 & \cdots & 2k-1 & 2k+1 \\ 3k+2 & 3k+1 & 3k & \cdots & 2k+3 & 2k+2 \\ 3k+3 & 3k+4 & 3k+5 & \cdots & 4k+2 & 4k+3 \end{pmatrix}.$$

回到原题.

由题意知 $n=3$ 符合条件.

故由引理知可经如下图方式得 $n=3900$ 或 $n=3903$ 满足分拆条件.



第二章　整数的相除

1. (1) 因为 $5|(x+9y)$，所以 $5|(2x+18y)$.

又 $(2x+18y)+(8x+7y)=10x+25y$.

由于 $5|(10x+25y)$，所以

$5|(8x+7y)$.

(2) 因为　$4(3x-7y+12z)+3(7x+2y-5z)=33x-22y+33z=11(3x-2y+3z)$，

显然 $11|11(3x-2y+3z)$，

又由已知 $11|(7x+2y-5z)$，于是

$11|(3x-7y+12z)$.

2. $2002\cdot2003\cdot\cdots\cdot4001\cdot4002$

$=(4003-2001)(4003-2000)\cdot\cdots\cdot(4003-2)(4003-1)$

$=4003n-1\cdot2\cdot3\cdot\cdots\cdot2000\cdot2001$.

从而有

$1\cdot2\cdot3\cdot\cdots\cdot2000\cdot2001+2002\cdot2003\cdot\cdots\cdot4002=4003n$，

即所给出的和数能被 4003 整除.

3. $1\cdot3\cdot5\cdot\cdots\cdot1983\cdot1985+2\cdot4\cdot6\cdot\cdots\cdot1984\cdot1986$

$=1\cdot3\cdot5\cdot\cdots\cdot1983\cdot1985+(1987-1985)(1987-1983)\cdot\cdots\cdot(1987-3)(1987-1)$

$=1\cdot3\cdot5\cdot\cdots\cdot1983\cdot1985+(-1985)(-1983)\cdot\cdots\cdot(-3)(-1)+1987$ 的倍数

$=1\cdot3\cdot5\cdot\cdots\cdot1983\cdot1985\cdot[1+(-1)^{993}]+1987$ 的倍数

$=1987$ 的倍数.

即 $1\cdot3\cdot5\cdot\cdots\cdot1983\cdot1985+2\cdot4\cdot6\cdot\cdots\cdot1984\cdot1986$ 能被 1987 整除.

4. 我们从能被 2^m-1 整除的，形如 $2^{k_1}+2^{k_2}+\cdots+2^{k_n}$ 的数中选取有最小的 n 的那些数. 再从所得的数中选取 $k_1+k_2+\cdots+k_n$ 最小的一个数，k_1，k_2，…，k_n 两两不等.

如果 $n\geqslant m$ 不成立，即 $n<m$，则 $k_i\leqslant m-1$.

$2^{k_1}+2^{k_2}+\cdots+2^{k_n}\leqslant2+2^2+\cdots+2^{m-1}=2^m-2<2^m-1$.

此时 $2^{k_1}+2^{k_2}+\cdots+2^{k_n}$ 不能被 2^m-1 整除，出现矛盾.

因此 $n\geqslant m$.

5. 一样多.

将小于 10000 的奇自然数 n 分成若干组，每组两个数(n_1, n_2)，且

$n_1+n_2=10000$.

由于 $n_1+n_2 \mid n_1^4+n_2^4$，

所以 $10000 \mid n_1^4+n_2^4$. ①

设 n_1^4 的后 4 个数码组成的数为 m_1，n_2^4 的后 4 个数码组成的数为 m_2，则由①得

$m_1+m_2=10000$.

由此可得 $n_1>m_1$ 等价于 $m_2>n_2$.

因此，题中所述的四位数一样多.

6. 由恒等式 $k^n-b^n=(k-b)(k^{n-1}+k^{n-2}b+\cdots+b^{n-1})$可得

$k-b \mid k^n-b^n$.

由已知 $k-b \mid k^n-a$，于是有

$k-b \mid (k^n-b^n)-(k^n-a)$，即 $k-b \mid a-b^n$.

由于 k 是不等于 b 的任意自然数，则 $k-b$ 为任意不等于零的整数，为使 $a-b^n$ 是任意不为零的整数的倍数，仅当 $a-b^n=0$，即 $a=b^n$.

7. 可以找到.

首先，我们任取 5 个自然数 a，b，c，d，e.

然后，再找一个整数 x，使

$(a+b+c+d+e) \mid x$.

构造 5 个新数

ax，bx，cx，dx，ex.

于是有

$(ax+bx+cx+dx+ex) \mid ax\cdot bx\cdot cx\cdot dx\cdot ex$.

这是因为

$$ax\cdot bx\cdot cx\cdot dx\cdot ex=abcde\cdot x^3\cdot(ax+bx+cx+dx+ex)\cdot\frac{x}{a+b+c+d+e},$$

而$\frac{x}{a+b+c+d+e}$是整数.

因而，为了得到所要求的 100 个自然数，可以先任取 100 个互不相同的自然数，求出其中每 5 个数的和，共得到 C_{100}^5 个和数，再找出一个能被这 C_{100}^5 个和数中的每一个都能整除的自然数 x（例如，将 x 取作这 C_{100}^5 个和数之积），然后用 x 去乘原来的 100 个数中的每一个，于是得到的 100 个新数即为所求.

8. 令 $x^{13}+x+90=(x^2-x+a)q(x)$，其中 a 为整数，$q(x)$ 是整系数多项式.

令 $x=-1$，0，1，则

$$\begin{cases}(a+2)q(-1)=88, & ①\\ aq(0)=90, & ②\\ aq(1)=92. & ③\end{cases}$$

由②，③得

$a[q(1)-q(0)]=2$，于是 $a\mid 2$.

因此 $a=1$ 或 2.

但当 $a=1$ 时，由①得

$3q(-1)=88$，这是不可能的.

故只能有 $a=2$.

当 $a=2$ 时，有

$x^{13}+x+90=(x^2-x+2)(x^{11}+x^{10}-x^9-3x^8-x^7+5x^6+7x^5-3x^4-17x^3-11x^2+23x+45)$.

9. 对任何一个数 a_i，我们都可以构造一个整除链

$a_i=a_{i_1}$，a_{i_2}，…，$a_{i_{m_i}}$

使得除 a_i 外，每个数都能被它前面的数整除，$a_i\geqslant 1$，称 a_i 为这个整除链的长度.

所有这种从 a_i 开始的整除链中，使 a_i 最大的，我们称之为从 a_i 开始的最大整除链，其长度记为 $A(i)$.

如果存在某个 i，使 $A(i)\geqslant n+1$，那么从 a_i 开始的最大整除链长 $\geqslant n+1$，取其前面的 $n+1$ 个数，则这 $n+1$ 个数中，除前面的一个数之外，每个数都能被它前面的数整除.

如果对每一个 i，$A(i)\leqslant n$，即 $A(1)$，$A(2)$，…，$A(mn+1)$ 都只能取 1，2，…，n 中的值，因此至少有 $\left[\frac{mn+1}{n}\right]+1$ 个相同.

设 $A(i_1)=A(i_2)=A(i_3)=\cdots=A(i_{m+1})=k$，$(1\leqslant k\leqslant n)$，则

a_{i_1}，a_{i_2}，…，$a_{i_{m+1}}$ 这 $m+1$ 个数中没有一个能被另一个整除.

这是因为，若 a_{i_2} 能被 a_{i_1} 整除，那么从 a_{i_2} 开始的最大整除链长 k，在它的前面加上一个数 a_{i_1}，则得到从 a_{i_1} 开始的一条整除链，长度为 $k+1$，那么 a_{i_1} 开始的最大整除链长 $\geqslant k+1$，与 $A(i_1)=k$ 矛盾. 这时，a_{i_1}，a_{i_2}，…，$a_{i_{m+1}}$ 是符合要求的 $m+1$ 个数.

10. 证法 1 对 A，B，C 赋值：设零件 A 为 1 分，零件 B 为 2 分，零件 C 为 4 分，则甲、乙、丙三种产品每件所需的零件分数之和都是 6. 库存三种零件的总分数之和应是

$6(p+q+r)+2+2$.

但此数不是 6 的倍数.

因此，组装成每件都为 6 分的产品，库存的零件必有剩余.

证法 2　组装成 p 件甲产品，q 件乙产品，r 件丙产品共需：

零件 A：$2p+2r$ 件，

零件 B：$2p+q$ 件，

零件 C：$q+r$ 件.

因此，加上剩余零件后，库存零件数为：A 有 $2p+2r+2$ 件，B 有 $2p+q+1$ 件，C 有 $q+r$ 件.

如果甲、乙、丙的件数分别改变成 x，y，z 件，于是可得方程组

$$\begin{cases}2x+2z=2p+2r+2,\\2x+y=2p+q+1,\\y+z=q+r,\end{cases}$$

解之得　$x=p+\frac{2}{3}$，$y=q-\frac{1}{3}$，$z=r+\frac{1}{3}$.

产品的件数应是非负整数，但解得的 x，y，z 都不是整数，由此说明，若要使 x，y，z 都取整数值，就不能把库存的三种零件都恰好用完.

11. 首先用数学归纳法证明：

设奇数 $a\geqslant 3$，对一切正整数 n，有

$$(1+a)^{a^n}=1+S_na^{n+1},\qquad ①$$

其中 S_n 是整数，且 $a\nmid S_n$.

对于 $n=1$，有

$$(1+a)^a=1+C_a^1a+C_a^2a^2+\cdots+C_a^aa^a=1+a^2(1+C_a^2+C_a^3a+\cdots+a^{a-2}).$$

由于 a 是奇数，所以 $a\mid C_a^2$，于是

$a\mid C_a^2+C_a^3a+\cdots+a^{a-2}$，从而

$a\nmid S_1=1+C_a^2+\cdots+a^{a-2}$.

因此，对 $n=1$，①式成立.

假设①式对自然数 $n=k_0$ 成立，则

$$\begin{aligned}(1+a)^{a^{k_0+1}}&=[(1+a)^{a^{k_0}}]^a\\&=(1+S_{k_0}a^{k_0+1})^a\\&=1+S_{k_0}a^{k_0+2}+C_a^2S_{k_0}^2a^{2k_0+2}+\cdots+S_{k_0}^aa^{a(k_0+1)}\\&=1+S_{k_0+1}a^{k_0+2},\end{aligned}$$

其中 $S_{k_0+1}=S_{k_0}+C_a^2S_{k_0}^2a^{k_0}+\cdots+S_{k_0}^aa^{a(k_0+1)-k_0-2}$.

由归纳假设 $a\nmid S_k$，因而 $a\nmid S_{k_0+1}$.

从而①式对 $n=k_0+1$ 成立.

即对一切自然数 n，①式成立.

类似地，可以证明：

设奇数 $b\geqslant 3$，则对一切正整数 n，有

$$(b-1)^{b^n}=-1+T_nb^{n+1},\qquad ②$$

其中 T_n 是整数，且 $b\nmid T_n$.

利用①，②可知，存在整数 S 和 T，使得

$1991\nmid S$，$1991\nmid T$，且

$1990^{1991^{1992}}+1992^{1991^{1990}}=T\cdot 1991^{1993}+S\cdot 1991^{1991}=1991^{1991}(T\cdot 1991^{2}+S)$.

由此，所求的最大的 $k=1991$.

12. 当 $n=1$，2，3 时，和式分别为 1，3，5，是整数.

当 $n>3$ 时，

$$\frac{n}{1!}+\frac{n}{2!}+\cdots+\frac{n}{(n-2)!}+\frac{n}{(n-1)!}+\frac{n}{n!}$$
$$=\frac{n(n-1)\cdots 2+n(n-1)\cdots 3+\cdots+n(n-1)+n+1}{(n-1)!}.$$

要使其为整数，分子一定能被 $n-1$ 整除，于是，$n+1$ 能被 $n-1$ 整除，即 $2[=n+1-(n-1)]$能被 $n-1$ 整除. 故 $n-1\in\{1,2\}$,不可能.

所以，和式为整数当且仅当 $n\in\{1,2,3\}$.

13. 首先证明：$(x+1)\mid(y^4-1)$.

设$\frac{x^4-1}{y+1}=\frac{a}{b}$，$\frac{y^4-1}{x+1}=\frac{c}{d}$，其中，$(a,b)=1$，$(c,d)=1$，且 b，$d>0$.

由条件知$\frac{ad+bc}{bd}$是整数.

于是，$b\mid d$,且 $d\mid b$,即 $b=d$.

又由$\frac{a}{b}\cdot\frac{c}{d}$是整数，$(a,b)=1,(c,d)=1$,知 $b=d=1$.

因此，$x+1$ 整除 y^4-1.

注意到$(y^4-1)\mid(y^{44}-1)$,$(x+1)\mid(x^4-1)$,则

$(x+1)\mid[x^4(y^{44}-1)+(x^4-1)]$,即$(x+1)\mid(x^4y^{44}-1)$.

14. 设 A，B 分别为 n 的前两位数字和后两位数字对应的两位数，则问题转化为求所有的(A,B),满足 $AB\mid(100A+B)$.

由于 $A\mid(100A+B)$,则 $A\mid B$.

令 $k=\frac{B}{A}$，因为 A，B 均为两位数，则 $10\leqslant A<\frac{100}{k}$，所以，$k<10$.

又 $AB\mid(100A+B)\Rightarrow kA^2\mid(100A+kA)\Rightarrow kA\mid(100+k)\Rightarrow k\mid(100+k)\Rightarrow k\mid 100$,

故 $k=1$，2，4，5.

又由 $A\left|\frac{100+k}{k}\right.$及 $10\leqslant A<\frac{100}{k}$，得

$(k,A)=(2,17)$或$(4,13)$.

故 $n=1734$ 或 1352.

15. 首先，经观察易知，当 $m=1$，$n=2$ 时，满足题意.

假设存在两个不同的正整数 m，n（不失一般性，不妨设 $m<n$）满足

$\frac{m+1}{n}+\frac{n+1}{m}=k(k\in\mathbf{N}_+)$，则

$k=\frac{1}{n}\left[\frac{n(n+1)}{m}+m+1\right]$,

故 $kn=\frac{n(n+1)}{m}+m+1$.

因此,$\frac{n(n+1)}{m}$为整数.

设 $r=\frac{n(n+1)}{m}$,则

$k=\frac{1}{n}(r+m+1)=\frac{1}{n}\left[r+\frac{n(n+1)}{r}+1\right]$.

故 $k=\frac{r+1}{n}+\frac{n+1}{r}$.

因此,若 (m,n) 为满足题意的数对,则 (n,r) 也为满足题意的数对.

又 $mr=n(n+1)>n^2$,及 $m<n$,则

$nr>n^2\Rightarrow r>n$.

因此,$n+r>m+n$.

综上,若 (m,n) 为满足题意的一个数对 $(m<n)$,则可造出一个新的数对 (n,r),使之也满足题意,且该数对的两元素之和比原来的大.因此,存在无限多个正整数对满足题目要求.

16. 注意到

$79\mid(a+77b)\Leftrightarrow79\mid(a-2b)\Leftrightarrow79\mid(39a-78b)\Leftrightarrow79\mid(39a+b)$,

$77\mid(a+79b)\Leftrightarrow77\mid(a+2b)\Leftrightarrow77\mid(39a+78b)\Leftrightarrow77\mid(39a+b)$,

故 $79\times77\mid(39a+b)$,

从而,$39a+b=79\times77k,k\in\mathbf{N}_+$.

注意到

$39a+39b=79\times77k+38b=(78^2-1)k+38b=(78^2-39)k+38(k+b)$,

所以,$39\mid(b+k)$,有 $b+k\geqslant39$.

从而,$39a+39b\geqslant(78^2-39)+38\times39$,即

$a+b\geqslant156-1+38=193$.

易知,$b=38$,$a=155$ 满足题设条件,因此,

$a+b=193$.

故$(a+b)_{\min}=193$.

17. 设 $a=\frac{m}{k}$,$b=\frac{n}{k}$(k 是 a,b 分母的最小公倍数).

设 $k>0$,$(k,m,n)=1$,于是

$S=\frac{m+n}{k}=\frac{m^2+n^2}{k^2}$,即

$(m+n)k=m^2+n^2$. ①

若存在素数可以整除 m,k,则也整除 n,矛盾.

同理,若存在素数可以整除 n,k,则也整除 m,也矛盾.

因此，$(k,m)=(k,n)=1$.

只要证明$(k,6)=1$，即证明$3\nmid k$，$2\nmid k$.

若$3\mid k$,则$3\nmid m$，$3\nmid n$，于是，

$m^2\equiv n^2=1(\bmod 3)$.

式①左边模3余0，右边模3余2，矛盾.

故$3\nmid k$.

若$2\mid k$,则$2\nmid m$，$2\nmid n$，于是，

$2\mid(m+n)$，$m^2\equiv n^2\equiv1(\bmod 4)$.

式①左边模4余0，右边模4余2，矛盾.

故$2\nmid k$.

18. 因为xy^2+2y整除$(2x+y)(xy^2+2y)-y(2x^2y+xy^2+8x)=2y^2-4xy$，

所以，$(xy+2)\mid(2y-4x)$.

下面考虑两种情况.

(1) 设$2y-4x\geqslant0$.

若$x\geqslant2$，则$xy+2>2y-4x$，于是，

$2y-4x=0$，即$x=a$，$y=2a$（其中，正整数$a\geqslant2$）.

经验证，$xy^2+2y=4a(a^2+1)$，$2x^2y+xy^2+8x=8a(a^2+1)$满足条件.

若$x=1$，则$(y+2)\mid(2y-4)$,即

$(y+2)\mid[2(y+2)-(2y-4)]=8\Rightarrow y=2$或6.

经验证，$y=2$满足条件，$y=6$舍去.

于是，解为$(a,2a)(a\in\mathbf{N}_+)$.

(2) 设$2y-4x<0$，即$4x-2y>0$.

若$y\geqslant4$，则$xy+2>4x-2y$，

于是，$y=1$，2或3.

若$y=1$，则$\frac{2x^2+9x}{x+2}=2x+5-\frac{10}{x+2}$是整数，因此，$x=3$或8.

若$y=2$，则$\frac{x^2+3x}{x+1}=x+2-\frac{2}{x+1}$是整数，因此，$x=1$.

若$y=3$，则$\frac{6x^2+17x}{9x+6}$是整数，于是，$3\mid x$.

设$x=3k(k\in\mathbf{N}^+)$，从而

$\frac{18k^2+17k}{9k+2}=2k+1+\frac{4k-2}{9k+2}$是整数．对于$k\geqslant1$是不可能的.

综上，所有解为$(a,2a)(a\in\mathbf{N}_+)$及$(3,1)$,$(8,1)$.

19. 我们指出，若$p(x)$为整系数多项式，则对任何非负整数r，正整数m、k，值$p(r)$与$p(mk+r)$被k除的余数相同.

考察$p(1)+p(2)+\cdots+p(k^2)$.

注意到，其中

$p(1), p(k+1), p(2k+1), \cdots, p((k-1)k+1)$

这 k 个加项被 k 除的余数相同，所以，它们的和能被 k 整除；

同理可知

$p(2), p(k+2), p(2k+2), \cdots, p((k-1)k+2)$

的和能被 k 整除；

如此下去，

$p(k), p(2k), p(3k), \cdots, p(k^2)$

的和能被 k 整除.

所以，$p(1)+p(2)+\cdots+p(k^2)$ 作为它们的总和能被 k 整除.

20. 设 $k=\prod\limits_{i=1}^{m} p_i^{a_i}$，其中，$p_1$，$p_2$，…，$p_m$ 为相异的素数，$a_i \in \mathbf{N}_+$.

由 $k \mid C_n^1=n$，得 $p_i^{a_i} \mid n(i=1,2,\cdots,m)$.

若 $p_i^{a_i} \parallel n$，则

$p_i^{a_i-1} \parallel C_n^{p_i}=\frac{n(n-1)\cdot\cdots\cdot(n-p_i+1)}{p_i(p_i-1)\cdot\cdots\cdot 2\cdot 1}$，

与 $k \mid C_n^{p_i}$ 矛盾.

故 $p_i^{a_i+1} \mid n$.

所以，$n=t\prod\limits_{i=1}^{m} p_i^{a_i+1} (t \in \mathbf{N}_+)$.

此时，$C_n^r=\frac{n(n-1)\cdot\cdots\cdot(n-r+1)}{r(r-1)\cdot\cdots\cdot 2\cdot 1}$ 的分子中 p_i 的次数不小于 $a_i+\sum\limits_{j=1}^{\infty}\left[\frac{r}{p_i^j}\right]$，分母中 p_i 的次数为 $\sum\limits_{j=1}^{\infty}\left[\frac{r}{p_i^j}\right]$.

于是，$p_i^{a_i} \mid C_n^r (i=1,2,\cdots,m)$.

故 $k \mid C_n^r (r=1,2,\cdots,n-1)$.

21. $A=\underbrace{\underbrace{142857}\underbrace{142857}\cdots\underbrace{142857}}_{k\text{个}}$，$k \in \mathbf{N}_+$.

设 $B=\overline{a_{n-1}\cdots a_1 a_0}$，则

$A=a_n 10^n+B$，$A_1=10B+a_n$，$B<10^n$.

令 $A_1=mA$，m 为正整数.

因为 $10^n m \leqslant Am=A_1<10^{n+1}$，故 $m<10$，从而，$A_1=mA$，即

$10B+a_n=m(a_n 10^n+B)$.

于是，$B=a_n\cdot\frac{10^n m-1}{10-m}$. ①

因为 A 的各位数字不全相等，所以，$A \neq A_1$，即 $m \neq 1$.

假设 $m \geqslant 5$，则

$B=a_n\cdot\frac{10^n m-1}{10-m} \geqslant 1\times\frac{5\times 10^n-1}{10-5}=10^n-\frac{1}{5}>10^n-1$.

所以，$B\geqslant10^n$，矛盾.

因此，$1<m<5$.

若 $m=2$，则 $B=a_n\cdot\dfrac{2\times10^n-1}{8}$.

又因为 $2\times10^n-1$ 是奇数，故 $8\mid a_n$，即 $a_n=8$.

但此时，$B\geqslant2\times10^n-1>10^n$，矛盾.

类似地，若 $m=4$，则 $B=a_n\cdot\dfrac{4\times10^n-1}{6}$，从而，$2\mid a_n$. 由此，

$B\geqslant\dfrac{4\times10^n-1}{3}>10^n$，矛盾.

这样，m 只可能有一个解 $m=3$.

由 $B=a_n\cdot\dfrac{3\times10^n-1}{7}<10^n$，解得 $a_n\leqslant2$.

若 $a_n=1$，则 $B=\dfrac{3\times10^n-1}{7}$，有

$A=\dfrac{1}{7}(10^{n+1}-1)$；

若 $a_n=2$，则 $B=2\times\dfrac{3\times10^n-1}{7}$，有

$A=\dfrac{2}{7}(10^{n+1}-1)$.

因为 A 为正整数，所以，$7\mid(10^{n+1}-1)$.

易知 $7\mid(10^m-1)$，当且仅当 $6\mid m$.

故 $n+1=6k$，$k\in\mathbf{N}_+$. 由此，

$A=\underbrace{142857142857\cdots142857}_{k个}$ 或 $A=\underbrace{285714285714\cdots285714}_{k个}$.

因为 $A_4=\overline{1\cdots}<\overline{2\cdots}=A$，即 A_4 不能被 A 整除，所以，第二种情况不可能.

另一方面，第一种情况为所求，这是因为易证明 142857 满足条件：

$428571=3\times142857$，$285714=2\times142857$，$857142=6\times142857$，

$571428=4\times142857$，$714285=5\times142857$.

于是，等式 $A_1=3A$，$A_2=2A$，$A_3=6A$，$A_4=4A$，$A_5=5A$ 也满足一般情况.

22. 首先证明 $4^{3^k\alpha}-1$ 恰能够被 3^{k+1} 整除，其中 k 和 α 是自然数，且 $3\nmid\alpha$.

我们用数学归纳法.

(1) $k=1$ 时，$4^{3\alpha}-1=64^{\alpha}-1=63(64^{\alpha-1}+\cdots+64+1)$.

由于 $64^{\alpha-1}+\cdots+64+1\equiv\alpha\not\equiv0\pmod 3$，则 $4^{3\alpha}-1$ 恰能被 $9=3^{1+1}$ 整除.

$k=2$ 时，$4^{9\alpha}-1=(4^9-1)[(4^9)^{\alpha-1}+\cdots+4^9+1]$.

由于 $4^9-1=64^3-1=63(64^2+64+1)$，则 $4^{9\alpha-1}$ 恰能被 $27=3^{2+1}$ 整除.

$k=3$ 时，$4^{27\alpha}-1=(4^{27}-1)[(4^{27})^{\alpha-1}+\cdots+4^{27}+1]$.

由于 $4^{27}-1=(4^9-1)[(4^9)^2+4^9+1]$，

而 4^9-1 恰能被 3^3 整除，$(4^9)^2+4^9+1$ 恰能被 3 整除，则 4^{27a} 1 恰能被 $81=3^{3+1}$ 整除.

(2) 假设 $4^{3^k a}-1$ 恰能被 3^{k+1} 整除，则

$4^{3^{k+1}a}-1=(4^{3^k a})^3-1=(4^{3^k a}-1)[(4^{3^k a})^2+4^{3^k a}+1]$.

由归纳假设知 $(4^{3^k a})^2+4^{3^k}+1$ 恰能被 3 整除，所以 $4^{3^{k+1}a}-1$ 恰能被 $3^{k+1}\cdot 3=3^{(k+1)+1}$ 整除.

于是对 $k+1$ 命题成立.

由于 4^m 4^n $4^n(4^{m-n}-1)$，则由上面的结论，当且仅当 m n 能被 3^k 整除时，4^m 4^n 能被 3^{k+1} 整除.

23. (1) 注意到

$$Z(a,b)=\frac{(3a)!\,(4b)!}{(a!)^4(b!)^3}=\frac{3(a)!}{a!\,(2a)!}\cdot\frac{(2a)!}{a!\,a!}\cdot\frac{(4b)!}{b!\,(3b)!}\cdot\frac{(3b)!}{b!\,(2b)!}\cdot$$

$$\frac{(2b)!}{(b-a)!\,(a+b)!}\cdot\frac{(a+b)!}{a!\,b!}\cdot(b-a)!=C_{3a}^{a}\cdot C_{2a}^{a}\cdot C_{4b}^{b}\cdot C_{3b}^{b}\cdot C_{2b}^{a+b}\cdot C_{a+b}^{a}\cdot(b-a)!.$$

这表明 $Z(a,b)$ 可表示为二项式系数和正整数 $(b-a)!$ 的乘积.

因此，当 $a\leqslant b$ 时，$Z(a,b)$ 是一个非负整数.

(2) 设 b 是给定的非负整数，p 是一个素数，且 $p>4b$. 令 $a=p$，考虑 $Z(p,b)$，恰好存在三个不大于 $3p$ 且能被 p 整除的正整数，即 $3p$、$2p$、p. 此外，$(4b)!$ 一定不能被 p 整除. 易知 p^3 是分子 $(3p)!\,(4b)!$ 的因子，而 p^4 不是分子 $(3p)!\,(4b)!$ 的因子.

另一方面，因为 $p|p!$，所以，p^4 一定是分母 $(p!)^4(b!)^3$ 的因子. 由此得出 $Z(p,b)$ 一定不是一个整数.

24. 由整除的性质 5(1)知，只需证明 $f(n,k)$ 不能被一个很小的自然数 n 整除.

由 $f(n,k)=3n^{2k}+3n^k-n^{2k}+n^k+10=3(n^{2k}+n^k+3)-n^k(n^k-1)(n^k+1)+1$，

及 $3|3(n^{2k}+n^k+3)$，$3|n^k(n^k-1)(n^k+1)$，$3\nmid 1$，

故 $3\nmid f(n,k)$. 因而 $f(n,k)$ 不能分解成三个或三个以上的连续自然数的乘积.

再证 $f(n,k)$ 不能分解成两个连续自然数的积.

由上知，$f(n,k)=3q+1(q\in\mathbf{N})$，因而只需证方程：$3q+1=x(x+1)$ 无正整数解. 而这一点可以分别具体验算 $x=3r,3r+1,3r+2$ 时，$x(x+1)$ 均不是 $3q+1$ 型的数来说明.

故 $f(n,k)$ 对任何自然数 n，k 都不能分解成若干个连续自然数之积.

第三章 同余

习题 A

1. 因 $47\equiv 7\pmod{10}$，$47^2\equiv 7^2\equiv 49\equiv -1\pmod{10}$，

$47^4\equiv(-1)^2\equiv 1\pmod{10}$. (*)

现考虑 $47^{47^{\cdots^{47}}}$ (k 个 47)的指数 $47^{\cdots^{47}}$ ($k-1$ 个 47)除以 4 的余数.

由于 $47\equiv -1\pmod 4$，所以

$47^{47^{\cdots^{47}}}$ ($k-1$ 个 47) $\equiv -1\equiv 3\pmod 3$.

于是由（*）式得

$47^{17^{\cdots^{47}}}$（k 个 47）$\equiv 47^3\equiv 7^3\equiv -7\equiv 3 \pmod{10}$.

故所求的个位数字是 3.

2. 由 $ab\equiv -1 \pmod{24}$ 得 $ab\equiv -1 \pmod 3$，所以 $a\not\equiv 0 \pmod 3$.

若 $a\equiv 1 \pmod 3$，则 $b\equiv -1 \pmod 3$；

若 $a\equiv -1 \pmod 3$，则 $b\equiv 1 \pmod 3$. 所以 $a+b\equiv 0 \pmod 3$.

同样有 $ab\equiv -1 \pmod 8$.

若 $a\equiv \pm 1 \pmod 8$，则 $b\equiv \mp 1 \pmod 8$；

若 $a\equiv \pm 3 \pmod 8$，且 $3ab\equiv -1 \pmod 8$，则 $\pm b\equiv -3 \pmod 8$，$b\equiv \mp 3 \pmod 8$.

所以 $a+b\equiv 0 \pmod 8$，于是 $a+b\equiv 0 \pmod{24}$，

即 $24\mid(a+b)$.

3. 由 $2222^{5555}\equiv 3^{5555}\equiv 3^4\equiv -1 \pmod 7$，

$5555^{2222}\equiv 4^{2222}\equiv 4^3\equiv 64\equiv 1 \pmod 7$，

故 $2222^{5555}+5555^{2222}\equiv -1+1\equiv 0 \pmod 7$.

4. 由 $8888^{2222}\equiv 8^{2222}\equiv 64^{1111}\equiv (-10)^{1111} \pmod{37}$，

$7777^{3333}\equiv 7^{3333}\equiv 343^{1111}\equiv 10^{1111} \pmod{37}$，

故 $8888^{2222}+7777^{3333}\equiv 0 \pmod{37}$.

5. 由 $(5,43)=1$，利用辗转相除法有 $5\cdot(-17)+43\cdot 2=1$，从而

$x\equiv(-17)\cdot 11\equiv -187\equiv -15\equiv 28 \pmod{43}$.

6. 因 $(111,321)=3$，且 $3\mid 75$，故同余式有 3 解.

先解同余式 $37x\equiv 25 \pmod{107}$.

$x\equiv\frac{75}{111}\equiv\frac{-32}{4}\equiv -8\equiv 99 \pmod{107}$，

从而 $x\equiv 99,\ 206,\ 313 \pmod{321}$ 为所求.

7. 由 $1\equiv 1 \pmod{11}$，$10\equiv -1 \pmod{11}$，$10^2\equiv(-1)^2\equiv 1 \pmod{11}$，$10^3\equiv(-1)^3\equiv -1 \pmod{11}$，…，$10^n\equiv(-1)^n \pmod{11}$，

于是，对于数 $A=\overline{a_na_{n-1}\cdots a_1a_0}$ 有

$$\begin{aligned}A&=a_0+a_1\cdot 10+a_2\cdot 10^2+\cdots+a_n\cdot 10^n\\&\equiv a_0-a_1+a_2-\cdots+(-1)^na_n\\&\equiv(a_0+a_2+a_4+\cdots)-(a_1+a_3+a_5+\cdots) \pmod{11}.\end{aligned}$$

因此，数 A 能否被 11 整除，就取决于

$(a_0+a_2+a_4+\cdots)-(a_1+a_3+a_5+\cdots)$

能否被 11 整除. 于是得判别法则：

将一个自然数 A 的奇数位的数字和与偶数位的数字和相减，当且仅当这个差被 11 整除，A 被 11 整除.

8. 因 $141x28y3\equiv 0 \pmod 9$，则

$141x28y3\equiv 1+4+1+x+2+8+y+3\equiv 0 \pmod 9$.

得 $x+y+1\equiv0\pmod 9$，即 $x+y\equiv8\pmod 9$，

于是可设 $x+y=9k+8$，从而有 $x+y=8$ 或 17.

又因 $141x28y3\equiv0\pmod{11}$，则

$141x28y3\equiv3+8+x+4-y-2-1-1\equiv0\pmod{11}$，

得 $x-y\equiv0\pmod{11}$，于是可设 $x-y=11l$，

从而有 $x-y=0$，而 $0\leqslant x$，$y\leqslant9$，故 $x=y=4$ 为所求.

9. 考虑模 3，若 $n\equiv0\pmod 3$，则 $n^2+n+2\equiv2\pmod 3$，

得 $3\nmid(n^2+n+2)$，即有 $15\nmid(n^2+n+2)$.

若 $n\equiv\pm1\pmod 3$，则 $n^2+n+2\equiv\pm1\pmod 3$，

得 $3\nmid(n^2+n+2)$，即有 $15\nmid(n^2+n+2)$.

10. 因为 $46^n+296\cdot13^n\equiv1^n+2\cdot1^n\equiv1+2\equiv0\pmod 3$，

$46^n+296\cdot13^n\equiv2^n-1\cdot2^n\equiv0\pmod{11}$，

又 n 是奇数，则

$46^n+296\cdot13^n\equiv(-13)^n+1\cdot13^n\equiv0\pmod{59}$ 且 $1947=3\cdot11\cdot59$，所以

$46^n+296\cdot13^n$（n 为奇数）被 1947 整除.

11. 因为 $1984=64\cdot31$，

故在 a_1，a_2，…，a_{65} 这 65 个互异的正整数中，至少有两数被 64 除的余数相同.

不妨设 $a_1=64k_1+r$，$a_2=64k_2+r$，$0\leqslant r<64$，则 $64\mid(a_1-a_2)$.

在 a_{66}，a_{67}，…，a_{97} 这 32 个互异正整数中，至少有两数被 31 除的余数相同.

不妨设 $a_{66}=31m_1+r$，$a_{67}=31m_2+r$，$0\leqslant r<31$，则 $31\mid(a_{66}-a_{67})$.

因为 $(64,31)=1$，所以

$1984\mid(a_1-a_2)(a_{66}-a_{67})$.

于是 a_1，a_2，a_{66}，a_{67} 即为所求的四个互异正整数.

12. 数 p 可化为

$p=\underbrace{11\cdots11}_{n个}(10^{3n}+9\cdot10^{2n}+8\cdot10^n+7)$.

由已知 $1987\mid\underbrace{11\cdots11}_{n个}$，则 $1987\mid p$.

数 q 可化为

$q=\underbrace{11\cdots11}_{n+1个}[10^{3(n+1)}+9\cdot10^{2(n+1)}+8\cdot10^{n+1}+7]$.

由 $10^n=9\cdot\underbrace{11\cdots11}_{n个}+1$ 及 $\underbrace{11\cdots11}_{n个}\equiv0\pmod{1987}$，则

$10^n\equiv1\pmod{1987}$.

又由 $10^{3(n+1)}=(10^n)^3\cdot1000$，$10^{2(n+1)}=(10^n)^2\cdot100$，$10^{n+1}=10^n\cdot10$，可得

$10^{3(n+1)}\equiv1000\pmod{1987}$，

$10^{2(n+1)}\equiv100\pmod{1987}$，

$10^{n+1}=10\pmod{1987}$.

从而可有

$10^{3(n+1)}+9\cdot 10^{2(n+1)}+8\cdot 10^{n+1}+7\equiv 1987\equiv 0 \pmod{1987}$.

于是 $1987\mid q$.

13. 设原式为 M，则

$$
\begin{aligned}
M&=2\cdot 2^{6k}+3\cdot 3^{6k}+5^{6k}+1\\
&=2\cdot 64^k+3\cdot 729^k+15625^k+1\\
&=2[(7\cdot 9+1)^k-1]+3[(7\cdot 104+1)^k-1]+[(7\cdot 2232+1)^k-1]+7.
\end{aligned}
$$

由于$(7a+1)^k\equiv 1 \pmod 7)$,则

$7\mid (7a+1)^k-1$.

于是　$7\mid M$.

14. $1971\equiv 0 \pmod 3$，所以，$1971^{26}\equiv 0 \pmod 3$.

又 $1972\equiv 1 \pmod 3$，所以

$1972^{27}\equiv 1^{27} \pmod 3$，

$1973\equiv 2 \pmod 3$，

$1973^{28}\equiv 2^{28} \pmod 3$.

于是有

$1971^{26}+1972^{27}+1973^{28}\equiv 2^{28}+1 \pmod 3$.

又 $2^{28}=4^{14}\equiv 1 \pmod 3$，所以

$2^{28}+1\equiv 2 \pmod 3$.

因此，$1971^{26}+1972^{27}+1973^{28}$不能被 3 整除.

15. 另一个数是 4.

由于每进行一步，黑板上的所有数的和模 11 的余数不变，且 $1+2+\cdots+2004\equiv 3 \pmod{11}$，$1000\equiv -1 \pmod{11}$，则另一个数一定模 11 余 4. 但是，在游戏过程中，写在黑板上的数都小于 11，1000 是黑板上原来的数，所以，另一个数一定是 4.

16. 令 $x=(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$.

只需证 3，4 均整除 x.

由抽屉原理知，a，b，c，d 四个数中至少有两个模 3 同余，这两个数之差必可被 3 整除，故 $3\mid x$.

若 a，b，c，d 四个数中有两个模 4 同余，则 $4\mid x$.

如若不然，a，b，c，d 模 4 的余数均不相等，此时，这四个余数必为两奇两偶，其差的乘积可被 4 整除，故仍有 $4\mid x$.

又因为$(3,4)=1$,故 $12\mid x$.

17. 当 $n=1$ 时，$3\nmid 1^{1987}=1$.

当 $n\geqslant 2$ 时，设 $a_n=1^{1987}+2^{1987}+\cdots+n^{1987}$，则

$$
\begin{aligned}
2a_n&=1^{1987}+2^{1987}+\cdots+n^{1987}+n^{1987}+\cdots+2^{1987}+1^{1987}\\
&=2+(n^{1987}+2^{1987})+[(n-1)^{1987}+3^{1987}]+\cdots+(n^{1987}+2^{1987}).
\end{aligned}
$$

由于对每一个 $k=2$，3，…

$n+2 \mid k^{1987}+(n+2-k)^{1987}$，

于是 $2a_n \equiv 2 (\mod n+2)$.

所以 a_n 不能被 $n+2$ 整除.

18. 设 $p=10a\pm b(a,b\in \mathbf{Z},1\leqslant b\leqslant 5)$，则

$p^2\equiv 10\cdot(\pm 2ab)+b^2 (\mod 100)$.

可以验证，当 $b=1$，3，4，5 时，p^2 的十位数字与个位数字的奇偶性相反；仅当 $b=2$ 时，p^2 的末两位数字奇偶性相同. 因此所求的 p 必须形如 $10a\pm 2$，而 $p=12$，$p^2=144$，末两位数字为 4.

依次计算 12^2，18^2，22^2，28^2，32^2，38^2，便知末二位数字非零且相同的最小正整数为 38.

19. 设 $b=a^2+a+1$，则

$(a^2+1)^3=(b-a)^3\equiv -a^3 (\mod b)$，　　①

$-a^3=-ab+a^2+a=-ab+b-1\equiv -1 (\mod b)$.　　②

于是由①，②可得

$(a^2+1)^3\equiv -1 \quad (\mod b)$.

因此有

$$\sum_{k=0}^{n} a_k (a^2+1)^{3k} \equiv \sum_{k=0}^{n}(-1)^k a_k (\mod b).$$

于是 $\sum\limits_{k=0}^{n} a_k(a^2+1)^{3k}$ 能被 $b=a^2+a+1$ 整除的充分必要条件是 $\sum\limits_{k=0}^{n}(-1)^k a_k$ 能被 a^2+a+1 整除.

若设 $c=a^2-a+1$，同样也可证明结论正确.

20. 由题意知

$3\mid 3^{31}+(3^{31}+1)+(3^{31}+2)+\cdots+(3^{31}+k)$，

$3\left|\left[(k+1)3^{31}+\frac{k(k+1)}{2}\right]\right.$，

于是 $3\left|\frac{k(k+1)}{2}\right.$，

从而 $3\mid k(k+1)$，即 $3\mid k$ 或 $3\mid k+1$，

即 $k\not\equiv 1 (\mod 3)$.

取 $k+1=6m$，即 $k=6m-1(m\in \mathbf{N})$就可得到符合题意的一列数.

令 $A_i=\{3^{31}+i,3^{31}+i+1,\cdots,3^{31}+i+5\}$.

由于$(3^{31}+i)+(3^{31}+i+5)=(3^{31}+i+1)+(3^{31}+i+4)=(3^{31}+i+2)+(3^{31}+i+3)$，

所以只要把 A_0，A_6，A_{12}，…，A_{6m-6} 每个集合中最大和最小的元素作为 A 的元素，第二大和第二小的元素作为 B 的元素，余下的作为 C 的元素即可得到所需的子集 A，B，C.

21. 设红片、黄片和蓝片的数目分别为 x，y，z，则 x，y，z 被 3 除的余数必有两个是相等的.

事实上，不妨设 $x=3a+1$，$y=3b+2$，$z=3c$，a，b，c 为整数，又

$x+y+z=3(a+b+c+1)\neq 1987$.

若 x，y，z 被 3 除的余数都相同，也导致矛盾.

假设 y 和 z 被 3 除同余，设

$x=3a+m$，$y=3b+n$，$z=3c+n$.

并不妨设 $c\geqslant b$.

若 $c=b$，则本题得证.

若 $c>b$，取黄片 $3b+n$，蓝片 $3b+n$. 按规则操作得红片数为 $3a+6b+m+2n$，黄片数为 0，蓝片数为 $3(c-b)$.

接着，各取 1 红片，1 蓝片，产生 2 黄片；再各取 2 黄片，2 蓝片，产生 4 红片，这时黄片仍为零，而蓝片减少了 3 片，即蓝片为 $3(c-b-1)$. 如果 $c-b-1=0$，本题得证，否则类似再操作 k 次，直至 $c-b-1-k=0$.

最后，所有玻璃片都涂上了红色.

最后产生 1987 片红片是因为红片数除以 3 的余数与蓝片、黄片除以 3 的余数不同，不论如何操作，都不可能改变三者的余数之间的关系，即两个相等而异于第三个，故最后变成哪一种颜色，与操作顺序无关.

22. 因

$$x^2+x+4=\left(x+\frac{1}{2}\right)^2+\left(\frac{3}{2}\right)^2+1^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2,$$

故 $n=5$ 是可以的. 下证 $n=4$ 不可以.

反证法. 若 $n=4$，设 $x^2+x+4=\sum\limits_{i=1}^{4}(a_ix+b_i)^2$，$a_i$，$b_i\in\mathbf{Q}$，则

$$\sum_{i=1}^{4}a_i^2=1,\sum_{i=1}^{4}a_ib_i=\frac{1}{2},\sum_{i=1}^{4}b_i^2=4.$$

$$\begin{aligned}故\frac{15}{4}&=\left(\sum_{i=1}^{4}a_i^2\right)\left(\sum_{i=1}^{4}b_i^2\right)-\left(\sum_{i=1}^{4}a_ib_i\right)^2\\&=(-a_1b_2+a_2b_1-a_3b_4+a_4b_3)^2+(-a_1b_3+a_3b_1-a_4b_2+a_2b_4)^2+\\&\quad(-a_1b_4+a_4b_1-a_2b_3+a_3b_2)^2.\end{aligned}$$

上式表明 $a^2+b^2+c^2=15d^2\equiv-d^2\pmod 8$ 有解.

不妨设 a，b，c，d 至少有一个奇数，且 a^2，b^2，c^2，$d^2\equiv0$，1，4 $\pmod 8$，上式显然无解，矛盾. 故 $n=4$ 不可以.

习题 B

1. 注意到

$S_i+T_i=x_1+x_2+\cdots+x_n$.

(1) 若 $x_1+x_2+\cdots+x_n\not\equiv0\pmod 3$，则

$m(2,1)=m(1,2)=0$.

(2) 若 $x_1+x_2+\cdots+x_n\equiv0\pmod 3$，则

$$\sum_{i=1}^{n}S_i=k(x_1+x_2+\cdots+x_n)\equiv0\pmod 3.$$

于是，在 S_r 中，被 3 除余 1 的个数与被 3 除余 2 的个数之差能被 3 整除，则

$3|m(2,1)-m(1,2)$.

即 $m(1,2)$ 与 $m(2,1)$ 被 3 除时余数相同.

2. 对于给定的正整数 $m\geqslant 2$，若整数 x 被 m 除得的余数为 i，$i\in\{0,1,\cdots,m-1\}$，则称 x 属于模 m 的剩余类 K_i.

设 A 的元素中属于 K_i 的数有 $n_i(i=0,1,2,\cdots,m-1)$ 个，而集合 $B=\{1,2,\cdots,n\}$ 的元素中属于 K_i 的数有 n_i' ($i=0$, 1, 2, …, $m-1$) 个，则

$$\sum_{i=0}^{m-1}n_i=\sum_{i=0}^{m-1}n'_i=n. \quad ①$$

易知，对任意 i，j，n_i' 与 n_j' 至多相差 1，且 $x-y$ 是 m 的倍数当且仅当两数 x，y 属于模 m 的同一个剩余类. 对于剩余类 K_i 中的任一对数 a_i，a_j，有 $m|a_j-a_i$，故属于 K_i 中 n_i 个数，共作成 $C_{n_i}^2$ 个 m 的倍数，考虑所有的 i，则

$$\overline{A}(m)=\sum_{i=0}^{m-1}C_{n_i}^2,$$

类似得 $B(m)=\sum_{i=0}^{m-1}C_{n_i'}^2$.

为证本题，只要证 $\sum_{i=0}^{m-1}C_{n_i}^2\geqslant\sum_{i=0}^{m-1}C_{n_i'}^2$，化简后，即要证

$$\sum_{i=0}^{m-1}n_i^2\geqslant\sum_{i=0}^{m-1}n_i'^2. \quad ②$$

据①易知，若对任意 i，j，$|n_i-n_j|\leqslant 1$，则 n_0，n_1，…，n_{m-1} 与 n_0'，n_1'，…，n_{m-1}' 就是同一组数（至多只有顺序不同），这时②式将取得等号.

若存在 i，j，使 $n_i-n_j\geqslant 2$，这时将 n_i，n_j 两数调整为 $\overline{n}_i$，$\overline{n}_j$，其中 $\overline{n}_i=n_i-1$，$\overline{n}_j=n_j+1$，其他元素不变，则

$n_i+n_j=\overline{n}_i+\overline{n}_j$.

由于 $(n_i^2+n_j^2)-(\overline{n}_i^2+\overline{n}_j^2)=2(n_i-n_j-1)>0$，

故调整后②式左边的和值将减少，因此②式取得最小值当且仅当 n_0，n_1，…，n_{m-1} 与 n_0'，n_1'，…，n_{m-1}' 为同一组数（至多只有顺序不同），即②成立，因此结论得证.

3. 证法 1　由带余除法定理可知，存在唯一的整数 q，r 使得

$p=3q+r$，其中 $0<r<3$.

取 $b_0=r$，那么

$\frac{p-b_0}{|b_0|}=\frac{3^{c_0}\cdot b_1^*}{|b_0|}$，其中 3 不整除 b_1^*，$0<b_1^*<\frac{p}{2}$；

取 $b_1=\pm b_1^*$ 满足条件 $b_1\equiv p(\mathrm{mod}\ 3)$，那么

$\frac{p-b_1}{|b_1|}=\frac{3^{c_1}\cdot b_2^*}{b_1^*}$，其中 3 不整除 b_2^*，$0<b_2^*<\frac{p}{2}$；

取 $b_2=\pm b_2^*$ 满足条件 $b_2\equiv p(\mathrm{mod}\ 3)$，那么

$\frac{p-b_2}{|b_2|}=\frac{3^{c_2}\cdot b_3^*}{b_2^*}$，其中 3 不整除 b_3^*，$0<b_3^*<\frac{p}{2}$；

一直做下去，我们就得到了

b_0，b_1，b_2，…，b_p.

这 $p+1$ 个整数均在 $\left(-\frac{p}{2},\frac{p}{2}\right)$ 之间，显然有两个数相等. 不妨设 $b_i=b_j$，$i<j$，而且 b_i，b_{i+1}，…，b_{j-1} 互不相同，那么

$$\frac{p-b_i}{|b_i|}\cdot\frac{p-b_{i+1}}{|b_{i+1}|}\cdot\cdots\cdot\frac{p-b_{j-1}}{|b_{j-1}|}=\frac{3^{c_i}\cdot b_{i+1}^*}{b_i^*}\cdot\frac{3^{c_{i+1}}\cdot b_{i+2}^*}{b_{i+1}^*}\cdot\cdots\cdot\frac{3^{c_{j-1}}\cdot b_j^*}{b_{j-1}^*}.$$

由于 $b_i=b_j$，从而 $b_i^*=b_j^*$，因此

上式 $=3^{c_i+c_{i+1}+\cdots+c_{j-1}}=3^n$，$n>0$.

让 b_i，b_{i+1}，…，b_{j-1} 按照从小到大的顺序排列，则原命题得证.

证法 2　分两种情形：

(1) $p=6k+1$，

$$\frac{p-1}{1}\cdot\frac{p+2}{2}\cdot\frac{p-4}{4}\cdot\frac{p+5}{5}\cdot\cdots\cdot\frac{p-(3k-2)}{3k-2}\cdot\frac{p+(3k-1)}{3k-1}=\frac{M}{Q},$$

其中 $Q=1\cdot2\cdot4\cdot5\cdot\cdots\cdot(3k-2)(3k-1)=\frac{(3k-1)!}{3^{k-1}(k-1)!}$，

$$\begin{aligned}M&=(p-1)\cdot(p+2)\cdot(p-4)\cdot(p+5)\cdot\cdots\cdot(p-(3k-2))(p+(3k-1))\\&=(p-3k+2)\cdot(p-3k+5)\cdot\cdots\cdot(p-1)\cdot(p+2)\cdot\cdots\cdot(p+(3k-1))\\&=(3k+3)\cdot(3k+6)\cdot\cdots\cdot(6k)\cdot(6k+3)\cdot\cdots\cdot(9k)\\&=3^{2k}\cdot(k+1)(k+2)\cdot\cdots\cdot(2k)\cdot(2k+1)\cdot\cdots\cdot(3k)\\&=3^{2k}\cdot\frac{(3k)!}{k!},\end{aligned}$$

所以 $\frac{M}{Q}=3^{3k}$，

因此，取

$\{a_1,a_2,\cdots,a_t\}=\{-3k+1,-3k+4,\cdots,-2,1,\cdots,3k-2\}$，就满足题目的要求.

(2) $p=6k+5$，

类似的有

$$\frac{p+1}{1}\cdot\frac{p-2}{2}\cdot\frac{p+4}{4}\cdot\frac{p-5}{5}\cdot\cdots\cdot\frac{p-(3k-1)}{3k-1}\cdot\frac{p-(3k+2)}{3k+2}=3^{3k+2}.$$

4. 对 $n=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$，$p_1$，…，$p_t$ 为互不相同的素数，$p_1^{\alpha_1}>\cdots>p_t^{\alpha_t}>1$，定义整数 b_n 如下：

$b_n\equiv p_2^{\alpha_2}\pmod{p_1^{\alpha_1}}$，$b_n\equiv p_3^{\alpha_3}\pmod{p_2^{\alpha_2}}$，…，$b_n\equiv p_t^{\alpha_t}\pmod{p_{t-1}^{\alpha_{t-1}}}$，$b_n\equiv0\pmod{p_t^{\alpha_t}}$ $(0\leqslant b_n<n)$.

令 $a_i=b_{n_i}$，若

$a_i+kn_i=a_j+ln_j$，

$n_i=p_{i1}^{\alpha_{i1}}\cdots p_{is}^{\alpha_{is}}$，$p_{i1}^{\alpha_{i1}}>\cdots>p_{is}^{\alpha_{is}}$，

$n_j=p_{j1}^{\beta_{j1}}\cdots p_{jr}^{\beta_{jr}}$，$p_{j1}^{\beta_{j1}}>\cdots>p_{jr}^{\beta_{jr}}$，

由条件知 $p_{i1}^{\alpha_{i1}}=p_{j1}^{\beta_{j1}}$，因此 $a_i\equiv a_j\pmod{p_{i1}^{\alpha_{i1}}}$，即 $p_{i2}^{\alpha_{i2}}\equiv p_{j2}^{\beta_{j2}}\pmod{p_{i1}^{\alpha_{i1}}}$.

而 $p_{i2}^{\alpha_{i2}}<p_{i1}^{\alpha_{i1}}$，$p_{j2}^{\beta_{j2}}<p_{j1}^{\beta_{j1}}$，故 $p_{i2}^{\alpha_{i2}}=p_{j2}^{\beta_{j2}}$，这样 $a_i\equiv a_j\pmod{p_{i2}^{\alpha_{i2}}}$. 同样有 $p_{i3}^{\alpha_{i3}}=p_{j3}^{\beta_{j3}}$，….

因此 $n_i = n_j$，矛盾.

所以 $\{a_i, a_i+n_i, a_i+2n_i, \cdots\}$ 两两不相交.

5. (1) 注意到 $\alpha+\beta=1$，$\alpha\beta=-1$，故

$\alpha^{n+2}-\beta^{n+2}=(\alpha+\beta)(\alpha^{n+1}-\beta^{n+1})-\alpha\beta(\alpha^n-\beta^n)=(\alpha^{n+1}-\beta^{n+1})+(\alpha^n-\beta^n)$，

两边除以 $\alpha-\beta$，就有 $a_{n+2}=a_{n+1}+a_n$.

(2) 由条件，可知 $b \mid a_1-2a$，即 $b \mid 1-2a$，而 $b>a$，故 $b=2a-1$. 并且对任意正整数 n，有 $b \mid a_n-2na^n$，$b \mid a_{n+1}-2(n+1)a^{n+1}$，$b \mid a_{n+2}-2(n+2)a^{n+2}$.

结合 $a_{n+2}=a_{n+1}+a_n$ 及 $b=2a-1$ 为奇数，可知

$b \mid (n+2)a^{n+2}-(n+1)a^{n+1}-na^n$.

而 $(b, a)=1$，所以

$$b \mid (n+2)a^2-(n+1)a-n. \qquad ①$$

在①中取 n 为 $n+1$，就有

$$b \mid (n+3)a^2-(n+2)a-(n+1). \qquad ②$$

将式①与式②右边相减，可知

$b \mid a^2-a-1$，即 $2a-1 \mid a^2-a-1$，故

$2a-1 \mid 2a^2-2a-2$.

而 $2a^2 \equiv a \pmod{2a-1}$，所以

$2a-1 \mid -a-2$，$2a-1 \mid -2a-4$.

故 $2a-1 \mid -5$，$2a-1=1$ 或 5.

但 $2a-1=1$ 导致 $b=a$ 矛盾，故 $2a-1=5$，$a=3$，进而 $b=5$.

下面证明：当 $a=3$，$b=5$ 时，对任意正整数 n，均有 $b \mid a_n-2na^n$，即 $5 \mid a_n-2n\times 3^n$.

当 $n=1$，2 时，由 $a_1=1$，$a_2=\alpha+\beta=1$，可知 $a_1-2\times 3=-5$，$a_2-2\times 2\times 3^2=-35$. 所以 $n=1$，2 时，有 $5 \mid a_n-2n\times 3^n$.

假设当 $n=k$，$k+1$ 时，结论成立，即

$5 \mid a_k-2k\times 3^k$，$5 \mid a_{k+1}-2(k+1)\times 3^{k+1}$，于是

$5 \mid (a_{k+1}+a_k)-2k\times 3^k-2(k+1)\times 3^{k+1}$，即 $5 \mid a_{k+2}-2\times 3^k(k+3(k+1))$.

故 $5 \mid a_{k+2}-2\times 3^k\times(4k+3)$.

为证明：$5 \mid a_{k+2}-2(k+2)\times 3^{k+2}$，我们只需证明

$$2(k+2)\times 3^{k+2} \equiv 2\times(4k+3)\times 3^k \pmod 5. \qquad ③$$

它等价于 $9(k+2) \equiv 4k+3$，即 $5k+15 \equiv 0 \pmod 5$，此式显然成立，于是③成立，从而结论对 $n=k+2$ 成立.

综上可知满足条件的 $(a,b)=(3,5)$.

注 题中所出现的数列 $\{a_n\}$ 为 Fibonacci 数列. 此题源于对 Fibonacci 数列性质的讨论. 关于 Fibonacci 数列的问题经常在数学竞赛中出现.

6. 我们先证明一引理：p 为奇素数，a，b，$n\in \mathbf{N}^*$，$p \mid a-b$，p 不整除 b，$a\neq b$，则 $p^\alpha \parallel n \Leftrightarrow p^\alpha \mid \dfrac{a^n-b^n}{a-b}$.

引理的证明：设 $a-b=l\cdot p^{\beta}$，p 不整除 l，$\beta\in\mathbf{N}^*$，则

$$\frac{a^n-b^n}{a-b}=\frac{1}{l\cdot p^{\beta}}((b+lp^{\beta})^n-b^n)$$

$$=\frac{1}{lp^{\beta}}(C_n^1lp^{\beta}b^{n-1}+\cdots+C_n^k(lp^{\beta})^kb^{n-k}+\cdots+(lp^{\beta})^n)$$

$$=nb^{n-1}+\cdots+\frac{n}{k}C_{n-1}^{k-1}l^{k-1}p^{\beta(k-1)}b^{n-k}+\cdots+l^{n-1}p^{\beta(n-1)}. \qquad ①$$

设 $p^{\gamma}\parallel n$，只需证明

$$p^{\gamma}\mid\frac{a^n-b^n}{a-b}. \qquad ②$$

因为 $p^{\gamma}\mid nb^{n-1}$，而对①式的其他项 $c_k\triangleq\frac{n}{k}C_{n-1}^{k-1}l^{k-1}p^{\beta(k-1)}b^{n-k}(k>1)$，

若能证得

$$p^{\gamma+1}\mid c_k(k>1), \qquad ③$$

即有②．欲证③，只需 $p^{\gamma+1}\mid\frac{n}{k}p^{\beta(k-1)}$ 既约后的分子

$$\Leftarrow p\mid\frac{p^{\beta(k-1)}}{k}\text{既约后的分子}, \qquad ④$$

而 $p^{\beta(k-1)}>(1+1)^{(k-1)}>1+(k-1)=k$，所以 $\frac{p^{\beta(k-1)}}{k}>1$，即 $\frac{p^{\beta(k-1)}}{k}$ 既约后分子大于 1，但其分子应为 p 的幂，所以④成立．引理得证．

下证原题．不妨设 $a=\frac{x}{z}$，$b=\frac{y}{z}$，x，y，z，$\in\mathbf{N}^*$ 且 $(x,y,z)=1$，

$$a^n-b^n\in\mathbf{Z}\Leftrightarrow z^n\mid x^n-y^n. \qquad ⑤$$

分两种情况：

(1) $z=2^k$，$k\in\mathbf{N}$，若 $k=0$，则 a，b 为正整数，原题得证．

若 $k\in\mathbf{N}^*$，设 $2^{\alpha}\mid x^2-y^2$，$\forall n\in\mathbf{N}^*$，$z^n\mid x^n-y^n$，设 $n=2^k\cdot l$，l 为奇数，则

$$2^n\mid x^n-y^n. \qquad ⑥$$

因为 $(x,y,z)=1$，所以 x，y 均为奇数，

$$x^n-y^n=x^{2^kl}-y^{2^kl}=(x^{2^k}-y^{2^k})(x^{2^k(l-1)})+\cdots+y^{2^k(l-1)}$$

$$=(x^2-y^2)(x^2+y^2)\cdots(x^{2^{k-1}}+y^{2^{k-1}})(x^{2^k(l-1)})+\cdots+y^{2^k(l-1)}).$$

注意到

$2^{\alpha}\parallel x^2-y^2$，$2\parallel x^2+y^2$，$2\parallel x^4+y^4$，…，$2\parallel x^{2^{k-1}}+y^{2^{k-1}}$，2 不整除 $x^{2^k(l-1)}+\cdots+y^{2^k(l-1)}$，所以 $2^{\alpha+(k-1)}\mid x^n-y^n$．结合⑥有 $n\leqslant\alpha+(k-1)$，但因为 $n=2^kl\geqslant2^k$，所以 $k\leqslant\log_2 n$，所以

$$n\leqslant\alpha+\log_2 n-1,$$

上式只能对有限多个 n 成立，矛盾．

(2) 存在奇素数 $p\mid z$．设 k 为满足 $p\mid x^k-y^k$ 的最小正整数，则若 $n\in\mathbf{N}^*$，$p\mid x^n-y^n$，即

$$x^n\equiv y^n(\bmod p)\Rightarrow(xy^{-1})^n\equiv1(\bmod p). \qquad ⑦$$

(y^{-1} 为 y 的数论倒数 mod p，下同)

因为 $x^k\equiv y^k \pmod p$，所以

$(xy^{-1})^k\equiv 1 \pmod p$. ⑧

由⑦，⑧熟知有 $k\mid n$.

设 $p^\alpha \parallel x^k-y^k$，$p^\beta \parallel \frac{n}{k}$，则

$\frac{n}{k}\geqslant p^\beta \Rightarrow \log_p n\geqslant \beta$. ⑨

由引理，$p^\beta \parallel \frac{x^n-y^n}{x^k-y^k}$，所以，$p^{\alpha+\beta}\parallel x^n-y^n$. 因为 $z^n\mid x^n-y^n$，所以 $p^n\mid x^n-y^n$，结合上面二式有

$n\leqslant \alpha+\beta\leqslant \alpha+\log_p n$（最后一个不等号可由⑨得到），

即 $n\leqslant \alpha+\log_p n$，

上式只能对有限个 n 成立. 矛盾.

综上可知，命题得证.

7. (1) 首先证明对任意 $m\in \mathbf{N}$，存在 $n\in \mathbf{N}$，使得 $m\mid f(n)$. 不妨设 $m>1$，令 $g(n)$ 是 $f(n)$ 除以 m 所得的余数，于是

$g(n)\in \{0, 1, 2, \cdots, m-1\}$ 且 $g(0)=0$，$g(1)=1$，

$g(n+2)\equiv 23g(n+1)+g(n) \pmod m, n=0,1,2,\cdots$. ①

考虑映射 T：$(f(n), f(n+1))\xrightarrow{T}(g(n), g(n+1))$.

由于 $(g(n), g(n+1))$ 仅有 m^2 个不同的取值，于是存在 n 与 n' 满足 $1\leqslant n<n'\leqslant m^2+1$，且 $(g(n), g(n+1))=(g(n'), g(n'+1))$ 即

$$\begin{cases}g(n+1)=g(n'+1),\\ g(n)=g(n').\end{cases}$$

由①推得 $g(n-1)=g(n'-1)$.

递推可得 $g(0)=g(n'-n)$.

由于 $g(0)=0$，所以 $g(n'-n)=0$，即 $m\mid f(n'-n)$，$n'-n\in \mathbf{N}$.

(2) 令 $c=\min\{n;\ n\in \mathbf{N},\ m\mid f(n)\}$.

下面证明：$m\mid f(n)\Leftrightarrow c\mid n$. ②

当 $m=1$ 时，显然 $c=1$，从而②成立；

当 $m>1$ 时，由于 $f(1)=1$，所以 $c>1$.

从而有

$m\mid f(0)=0$，

$m\mid f(c)$，但 $m\nmid f(n)$，$n<c$. ③

为证明②，我们用数学归纳法证明如下的命题：设 $k\in \mathbf{N}$，且 $m\mid f(k)$，则

$f(k+t)\equiv(-1)^{t+1}f(k-t) \pmod m$. ④

对任意 $t\in \mathbf{N}$，且 $t\leqslant k$.

(i) 当 $t=1$ 时，由于 $f(k)\equiv 0 \pmod m$，从而由递推公式可知

$f(k+1)=23f(k)+f(k-1)\equiv f(k-1) \pmod{m}$.

即 $t=1$ 时，④成立.

(ii) 设 $1\leqslant t\leqslant s$ 时，④成立，其中 $s\in\mathbf{N}$，且 $s<k$.

由递推公式及归纳假设知

$$f(k+s+1)=23f(k+s)+f(k+s-1)\equiv(-1)^{s+1}23f(k-s)+(-1)^{s}f(k-(s-1)) \pmod{m}.$$

又

$$\begin{aligned}(-1)^{s+1}23f(k-s)+(-1)^{s}f(k-(s-1))&=(-1)^{s}[f(k-(s-1))-23f(k-s)]\\&=(-1)^{s+2}f(k-(s+1)),\end{aligned}$$

所以 $f(k+s+1)\equiv(-1)^{s+2}f(k-(s+1)) \pmod{m}$.

因此，当 $t=s+1$ 时，④成立.

综合③、④即可得②.

以下利用②证明所要的结果.

事实上，对任意 $m\in\mathbf{N}$，由②知，存在 $c\in\mathbf{N}$，使得

$m \mid f(n)\Leftrightarrow c \mid n$.

对于 $c \mid n$，再由②可知，存在 $d\in\mathbf{N}$，使得

$c \mid f(n)\Leftrightarrow d \mid n$.

于是 $m\mid f(f(n))\Leftrightarrow c\mid f(n)\Leftrightarrow d\mid n$.

8. 因为 2 是素数，所以本题等价于求自然数 $n>3$，使

$1+C_n^1+C_n^2+C_n^3=2^k$ ($k\in\mathbf{N}$，$k\leqslant2000$).

$$1+C_n^1+C_n^2+C_n^3=1+n+\frac{n(n-1)}{2}+\frac{n(n-1)(n-2)}{6}=\frac{(n+1)(n^2-n+6)}{6},$$

有 $(n+1)(n^2-n+6)=3\times2^{k+1}$.

作代换 $m=n+1$，得

$$m(m^2-3m+8)=3\times2^{k+1}. \qquad ①$$

下面对 m 分类讨论.

(1) 若 $m=2^s$ ($m>4$，$s\geqslant3$)，则

$m^2-3m+8=3\times2^t$ ($t\in\mathbf{N}$).

如果 $s\geqslant4$，那么 $m^2-3m+8=3\times2^t\equiv8 \pmod{16}$.

由此可知，$t=3$，从而

$m^2-3m+8=24$，即 $m(m-3)=16$. 这不可能.

所以只有 $s=3$，$m=8$，即 $n=7$.

(2) 若 $m=3\times2^u$ ($m>4$，$u\geqslant1$)，则

$m^2-3m+8=2^v$ ($v\in\mathbf{N}$).

如果 $u\geqslant4$，则

$m^2-3m+8=2^v\equiv8 \pmod{16}$.

由此可知，$v=3$，故 $m(m-3)=0$. 这也不可能.

又 $u=1$ 和 $u=2$ 时，即 $m=3\times2$ 和 $m=3\times2^2$ 时，都不能使 $m^2-3m+8=2^v$ 成立.

当 $m=3\times2^3=24$ 时，可求出 $n=23$.

因 $1+C_7^1+C_7^2+C_7^3=64=2^6 \mid 2^{2000}$，且 $1+C_{23}^1+C_{23}^2+C_{23}^3=2^{11} \mid 2^{2000}$。
故本题答案为 $n=7$ 和 $n=23$。
9. 对于 $h=2^r$，约定将满足题目条件的所有的 k 的集合记为 $k(h)$。
下面我们证明：$k(h)=\{2^{r+s}t \mid s, t\in \mathbf{N}, 2\nmid t\}$。
先证明下面的事实：

$$m\equiv 1 \pmod 4 \Rightarrow 2^r \parallel \frac{m^{2^r}-1}{m-1}.$$

这个事实是显然的，这是因为

$$\frac{m^{2^r}-1}{m-1}=(m^{2^{r-1}}+1)(m^{2^{r-2}}+1)\cdot \cdots \cdot (m^2+1)(m+1).$$

由于 $m\equiv 1 \pmod 4$，则 $m^{2^u}+1\equiv 2 \pmod 4$，其中 $u=0, 1, \cdots, r-1$。
因此，$2^r \ \frac{m^{2^r}-1}{m-1}$，$2^{r+1}\nmid \frac{m^{2^r}-1}{m-1}$，即 $2^r \parallel \frac{m^{2^r}-1}{m-1}$。
(1) 先证明：若 $s\geqslant 2$，$2\nmid t$，则 $k=2^{r+s}t\in k(h)$。
事实上，存在 $m=2^s t+1$，$n=m-1$，使得 $2^r \parallel \frac{m^{2^r}-1}{m-1}$。
由于 $\frac{m^k-1}{k}=\frac{m^{2^r}-1}{2^{r+s}t}=\frac{m^{2^r}-1}{2^r\cdot 2^s t}=\frac{m^{2^r}-1}{2^r(m-1)}$ 是奇自然数，所以 $k \mid m^k-1$。
又 $n^{\frac{m^k-1}{k}}=(m-1)^{\frac{m^k-1}{k}}\equiv -1 \pmod m$，所以

$$m \mid n^{\frac{m^k-1}{k}}+1.$$

(2) 再证明：对于 $2\nmid t$，$k=2^{r+1}t\in k(h)$。
事实上，存在 $m=4t^2+1$，$n=2t$，使得

$$\frac{m^k-1}{k}=\frac{m^{2^r}-1}{2^r(m-1)}\cdot 2t,$$

$$n^{\frac{m^k-1}{k}}=(n^2)^{\frac{m^{2^r}-1}{2^r(m-1)}\cdot t}\equiv -1 \pmod m.$$

所以 $k \mid m^k-1$，$m \mid n^{\frac{m^k-1}{k}}+1$。
(3) 用反证法证明：对于 $0\leqslant q\leqslant 2r$，$2\nmid t$，$2^q t\notin k(h)$。
若对 $k=2^q t$，有 m，n 满足题目中的要求，显然 m 与 n 互素。
在 m 的所有素因数中，取以下表示中指数 a 最小的一个素数 p：$p=2^a b+1$，$2\nmid b$。
易见 $2^a \mid m-1$。
一方面，由 $p \mid n^{\frac{m^k-1}{k}}+1$ 有

$$\left(n^{\frac{m^k-1}{2^q t}}\right)^b\equiv -1 \pmod p. \qquad (※)$$

另一方面，因为 $2^a \mid m-1$，$2^{q+a} \mid m^k-1$，所以有

$$\left(n^{\frac{m^k-1}{2^q t}}\right)^b=\left(n^{\frac{m^k-1}{2^{q+a}t}}\right)^{2^a\cdot b}\equiv\left(n^{\frac{m^k-1}{2^{q+a}t}}\right)^{p-1}\equiv 1 \pmod p. \qquad (※※)$$

(※) 与 (※※) 矛盾. 由(1),(2),(3),对于 $h=2^r$，有
$k(h)=\{2^{r+s}t \mid s, t\in \mathbf{N}, 2\nmid t\}$。

10. 所求 A 为 $\{3l+2 \mid 0\leqslant l\leqslant 9\}$.

设 A 满足题中条件且 $|A|$ 最大. 因为两个相邻整数之积被 30 除，余数为 0，2，6，12，20，26，则对任一 $a\in A$，有 $2a\not\equiv 0, 2, 6, 12, 20, 26 \pmod{30}$，即 $a\not\equiv 0, 1, 3, 6, 10, 13, 15, 16, 18, 21, 25, 28$，因此，$A\subseteq\{2, 4, 5, 7, 8, 9, 11, 12, 14, 17, 19, 20, 22, 23, 24, 26, 27, 29\}$，后一集合可分拆成下列 10 个子集的并，其中每一个子集至多有一个元素包含在 A 中：$\{2, 4\}$，$\{5, 7\}$，$\{8, 12\}$，$\{9, 11\}$，$\{14, 22\}$，$\{17, 19\}$，$\{20\}$，$\{23, 27\}$，$\{24, 26\}$，$\{29\}$，故 $|A|\leqslant 10$.

若 $|A|=10$，则每个子集恰好有一个元素包含在 A 中，因此 $20\in A$，$29\in A$.

由 $20\in A$ 知 $12\notin A$，从而 $8\in A$，这样 $4\notin A$，$22\notin A$，$24\notin A$，因此 $2\in A$，$14\in A$，$26\in A$.

由 $29\in A$ 知 $7\notin A$，$27\notin A$，从而 $5\in A$，$23\in A$，这样 $9\notin A$，$19\notin A$，因此 $11\in A$，$17\in A$.

综上有 $A=\{2, 5, 8, 11, 14, 17, 20, 23, 26, 29\}$，此 A 确实满足要求.

11. 由已知，$\frac{(b+1)(a+b-1)}{a^2+b+1}=\frac{b^2-a^3-1}{a^2+b+1}+a$ 也是整数.

设 $p^k=m=a^2+b+1$，k 为正整数，则 $p^k \mid (b+1)(a+b-1)$.

若 p 不整除 $b+1$，$a+b-1$ 之一，则 p^k 必整除另一个，但此时 $p^k=a^2+b+1>\max\{b+1, a+b-1\}$，矛盾！故

$b+1\equiv a+b-1\equiv 0 \pmod p$，

$a^2=p^k-(b+1)\equiv 0 \pmod p$.

由于 p 为素数，有

$a\equiv 0 \pmod p$，

$0\equiv(b+1)-(a+b-1)+a\equiv 2 \pmod p\Rightarrow p=2$.

设

$$\begin{cases}a^2+b+1=2^k,\\ b+1=2^{k_1}t_1,\\ a+b-1=2^{k_2}t_2,\\ k_1+k_2\geqslant k,\\ k>2k_2,\end{cases}$$

其中 t_1，t_2 为奇数，k_1，k_2 为正整数，最后一式由 $m\nmid(a+b-1)^2$ 可知.

由于 $2^k=a^2+b+1>b+1=2^{k_1}t_1$，故还可得到

$k>k_1$.

(i) 当 $k_1\geqslant 3$，

因为 $a^2=2^k-2^{k_1}t_1\equiv 0 \pmod{2^3}$，故

$a\equiv 0 \pmod 4$，$a+b-1\equiv 0-1-1\equiv 2 \pmod 4$.

由此必有 $k_2=1$. 由 $k_1+k_2\geqslant k>k_1$ 知，$k=k_1+1$. 此时 $2^{k_1}t_1=b+1<a^2+b+1=2^k=2^{k_1+1}$，故

t_1-1.

于是

$$\begin{cases}b+1=2^{k_1},\\a^2+b+1=2^{k_1+1}\end{cases}\Rightarrow\begin{cases}a=2^x,\\b=2^{2x}-1,\end{cases}$$

这里仅当 k_1 为偶数时才有对应解（因出现了 a^2），故设 $k_1=2x$，则 $(a,b)=(2^x,2^{2x}-1)$ 为一组通解. 检验知，当 $x=1$ 时，$(a,b)=(2,3)$，但 $\frac{(a+b-1)^2}{a^2+b+1}=2$ 为整数，故舍去；对 $x\geqslant2$，数组均满足所有条件.

(ii) 当 $k_1=2$，

由 $k>k_1$ 知，$k\geqslant3$.

由 $k_1+k_2\geqslant k$ 及 $k>2k_2$ 知，

$2k_2<k\leqslant k_2+2\Rightarrow k_2<2$，

继而有 $k\leqslant3$，故

$k=3$.

但

$$\begin{cases}b+1=2^2t_1,\\a^2+b+1=8\end{cases}\Rightarrow\begin{cases}t_1=1,\\a=2,\\b=3,\end{cases}$$

舍去.

(iii) 当 $k_1=1$，则

$2k_2<k\leqslant k_2+1\Rightarrow k_2<1$，矛盾！

综上，所求数组 (a,b) 为 $(2^x,2^{2x}-1)$ $(x=2,3,4,\cdots)$.

第四章　奇数与偶数

1. (1) 当 $n=3$ 时，存在满足题意的安排. 具体安排如下（把 9 位女同学记为 1，2，…，9）：

(1,2,3),(1,4,5),(1,6,7),(1,8,9),(2,4,6),(2,7,8),

(2,5,9),(3,4,8),(3,5,7),(3,6,9)(4,7,9),(5,6,8).

(2) 任意取一位女同学，因为她和其他每一位女同学恰好值勤一次，并且每天有三人值勤，所以其余 $3n-1$ 位女同学可两两配成对，故

$2\mid 3n-1$，

所以 n 是奇数.

注　第(1)小题是一个结论开放的问题，问是否存在满足题意的安排. 如果存在的话，我们就要构造具体的例子（见我们给出的例子）；如果不存在，那么就要给出证明（常常是用反证法）.

2. 题中的方程就是

$n?=32=2(n-8)$. ①

由于 $n?$ 不能被 4 整除，故由式①推知，$n-8$ 为奇数. 设 $n>9$，则 $n-8$ 具有奇数素因数 p. 由于 $p<n$，所以 p 能够整除 $n?$. 这就意味着 32 可被 p 整除，而这是不可能的.

由上可知 $n\leqslant 9$ 且为奇数．当 $n=9$ 时，有 $n?\ -210>2.9+16.7$，显然是我们方程的根．而当 $n=5$ 时，却有 $n?\quad 6<2\times 5+16$．所以我们的方程有唯一的根 $n=7$．

3．由于乘积

$x_1x_2x_3x_4$，$x_2x_3x_4x_5$，…，$x_nx_1x_2x_3$

都是 $+1$ 或 -1，且其总和为 0，所以一定共有偶数项，即 n 一定是偶数 $2m$．

将上面的 n 个数相乘，一方面，其中的 $+1$ 和 -1 各有 m 个，所以它们的乘积为 $(-1)^m$．

另一方面，在乘积中，x_1，x_2，…，x_n 作为因数都出现四次，所以乘积为 $+1$，于是

$(-1)^m=1$，m 为偶数．

因此 n 是 4 的倍数．

4．(1) 因为 a_0 为奇数，所以，由 a_n 递推关系式知 $\{a_n\}$ 的每一项均为奇数．

设 $(a_k,\ a_n)=m\ (k<n)$．

下面证明：$m=1$．

因为 $a_n-2=a_0a_1\cdots a_k\cdots a_{n-1}$，所以，

$m\mid 2$．

若 $m=2$，则 a_k，a_n 均为偶数，矛盾．

故 $m=1$．

(2) 因为 $a_{n-1}-2=a_0a_1\cdots a_{n-2}$，所以，

$a_n-2=(a_{n-1}-2)a_{n-1}$，即 $a_n-1=(a_{n-1}-1)^2$．

因此，$a_n-1=(a_{n-1}-1)^2=(a_{n-2}-1)^4=\cdots=(a_{n-k}-1)^{2^k}=\cdots=(a_0-1)^{2^n}=2^{2^n}$，

即 $a_n=2^{2^n}+1$．

因此，$a_{2007}=2^{2^{2007}}+1$．

5．设 k 是十进制数，s 是 k 的各位数字之积．

易知 $s\in\mathbf{N}$，故 $8\mid k$ 且 $\dfrac{25}{8}k-211\geqslant 0$，即

$k\geqslant\dfrac{1688}{25}$．

因为 $k\in\mathbf{N}_+$，所以，$k\geqslant 68$．

又 $8\mid k$，故 k 的个位数是偶数．从而，s 是偶数．

由于 211 是奇数，故 $\dfrac{25}{8}k$ 为奇数，所以，$16\nmid k$．

设 $k=\overline{a_1a_2\cdots a_t}$，$0\leqslant a_i\leqslant 9\ (i=2,3,\cdots,t)$，$1\leqslant a_1\leqslant 9$．由定义，

$$S=\prod_{i=1}^{t}a_i\leqslant a_1\times 9^{t-1}<a_1\times 10^{t-1}=\overline{a_1\underbrace{00\cdots 0}_{t-1\text{个}}}\leqslant k,$$

故 $k>s=\dfrac{25}{8}k-211$，所以，$k\leqslant 99$．

由 $8\mid k$，$16\nmid k$，得 $k=72$ 或 88．

经检验，k 为 72 或 88．

6. 设 $x+y=2^a$，$xy+1=2^b$.

若 $xy+1\geqslant x+y$，则 $b\geqslant a$.

于是，有 $xy+1\equiv 0 \pmod{2^a}$.

又因为 $x+y\equiv 0 \pmod{2^a}$，所以，

$-x^2+1\equiv 0 \pmod{2^a}$，即 $2^a \mid (x+1)(x-1)$.

由于 $x+1$ 与 $x-1$ 只能均为偶数，且 $(x+1,x-1)=2$，从而，一定有一个能被 2^{a-1} 整除.

由于 $1\leqslant x\leqslant 2^a-1$，所以，

$x=1$，$2^{a-1}-1$，$2^{a-1}+1$ 或 2^a-1.

相应地，$y=2^a-1$，$2^{a-1}+1$，$2^{a-1}-1$ 或 1 满足条件.

若 $x+y>xy+1$，则有 $(x-1)(y-1)<0$，矛盾.

综上所述，

$$\begin{cases}x=1,\\y=2^a-1;\end{cases}\begin{cases}x=2^b-1,\\y=2^b+1;\end{cases}\begin{cases}x=2^c+1,\\y=2^c-1;\end{cases}\begin{cases}x=2^d-1,\\y=1.\end{cases}$$

其中 a，b，c，d 为任意正整数.

7. 用数学归纳法证明，对每个正整数 n，有唯一的由十进制表示的仅包含数字 2 和 5 的 n 位的正整数 x_n，能被 2^n 整除.

当 $n=1$，2，3 时，$x_1=2$，$x_2=52$，$x_3=552$，结论显然成立.

假设 x_n 是唯一由数字 2 和 5 表示且能被 2^n 整除的 n 位的正整数.

考察数字

$2\times 10^n+x_n$，$5\times 10^n+x_n$.

这两个数都是在数 x_n 的左边加上数字 2 或 5 得到的，它们都是由 2 和 5 表示，且有 $n+1$ 位.

因为 x_n 和 10^n 能被 2^n 整除，所以，这两个数均能被 2^n 整除.

注意到

$$\frac{5\times 10^n+x_n}{2^n}-\frac{2\times 10^n+x_n}{2^n}=3\times 5^n.$$

由于差为奇数，因此，$\frac{5\times 10^n+x_n}{2^n}$ 和 $\frac{2\times 10^n+x_n}{2^n}$ 之中恰有一个为偶数.

这就证明了数字 $2\times 10^n+x_n$ 和 $5\times 10^n+x_n$ 恰有一个能被 2^{n+1} 整除，即 x_{n+1} 满足所有的条件.

下面证明 x_{n+1} 的唯一性.

为此，去掉 x_{n+1} 最左边的一位，得到一个仅包含数字 2 和 5 且能被 2^n 整除的 n 位数 x_n，由归纳假设，x_n 为满足条件的唯一值. 因此，x_{n+1} 的形式一定是 $2\times 10^n+x_n$ 或 $5\times 10^n+x_n$.

于是，根据上面的证明恰好其中一个是满足条件的 x_{n+1}.

8. 若不然，设黑色正方形上的石头的数目为奇数，将 14 列依次编号为 1，2，…，14，将编号为奇数的列称为奇列，编号为偶数的列称为偶列. 对各行也类似处理. 由于对称性，不防设黑格是奇行奇列格和偶行偶列格.

设奇行奇列格中有 k_1 个中放有奇数块石头，偶行偶列格中有 k_2 个中放有奇数块石头，奇行偶列格中有 k_3 个中放有奇数块石头.

由奇行中有奇数块石头，有 $k_1+k_3\equiv1\pmod 2$.

由偶列中有奇数块石头，有 $k_2+k_3\equiv1\pmod 2$.

由反证假设，有 $k_1+k_2\equiv1\pmod 2$.

相加得 $2(k_1+k_2+k_3)\equiv1\pmod 2$，这不可能.

因此，黑色正方形上石头的数目共有偶数个.

9. 假设存在这样的直角三角形.

设两直角边长度分别为 x，y，则

$x^2+y^2=2006$.

又 2006 为偶数，故 x，y 的奇偶性相同.

若 x，y 均为偶数，则必有 $4\mid(x^2+y^2)$，但 $4\nmid2006$. 所以，x，y 均为奇数.

设 $x=2k+1$，$y=2l+1$（k，l 为非负整数），则原方程化为

$(2k+1)^2+(2l+1)^2=2006$，

化简得

$k(k+1)+l(l+1)=501$.

对于任何整数 n，$n(n+1)$ 为偶数，故上式左边为偶数，而右边为奇数，矛盾.

因此，这样的三角形不存在.

10. 一切奇数.

如果正整数 n 为奇数，则只需令

$a=\frac{1}{2}$，$b=\frac{2^n-1}{2}$.

事实上，$a+b$ 是整数，而

$a^n+b^n=(a+b)(a^{n-1}-a^{n-2}b+\cdots+b^{n-1})=2^{n-1}(a^{n-1}-a^{n-2}b+\cdots+b^{n-1})$，

由于括号中每一项的分母都是 2^{n-1}，所以，a^n+b^n 也是整数.

现设正整数 n 为偶数，即 $n=2k$（$k\in\mathbf{N}_+$）.

如果能够找到所说的正有理数 a，b，那么，由于 $a+b$ 是整数，所以，它们的既约分数表达式中的分母相同，即有 $a=\frac{p}{d}$，$b=\frac{q}{d}$，并且 $p+q$ 可被 d 整除. 同时，有

$$p^n+q^n=(p^{2k}-q^{2k})+2q^{2k}=(p^2-q^2)(p^{2k-2}+p^{2k-4}q^2+\cdots+q^{2k-2})+2q^{2k}=(p+q)K+2q^{2k},$$

其中，$K=(p-q)(p^{2k-2}+p^{2k-4}q^2+\cdots+q^{2k-2})$ 是一个整数.

注意到，$a^n+b^n=\frac{p^n+q^n}{d^n}$ 也是整数，亦即 p^n+q^n 能被 d^n 整除，特别地，能被 d 整除.

又由于 d $(p+q)$，所以，$d\mid2q^n$.

但 $\frac{q}{d}$ 是既约分数，所以，$d\mid2$，即 $d=2$.

故 p^n，q^n 都是奇数的平方，它们被 4 除的余数都是 1.

因此，p^n+q^n 不能被 4 整除.

但是，如前所证 p^n+q^n 能被 $d^n=2^n=2^{2k}$ 整除，显然是 4 的倍数. 矛盾.

11. 若 $k=4t+1$，$t\in\mathbf{N}$，显然满足要求. 取 $4t+1$ 及 $2t$ 个 1，$2t$ 个 -1 即可.

若 $k=4$，则 $a_1a_2a_3a_4=4$. 只可能是 $a_1=4$ 或 $a_1=a_2=2$，显然无解.

若 $k=4t$，$t\geqslant 2$，分两种情况讨论.

当 t 为奇数时，取 $2t$，-2，x 个 1，y 个 -1（x，y 待定），则 $\begin{cases}x+y=4t-2,\\x-y+2t-2=4t.\end{cases}$

解得 $x=3t$，$y=t-2$.

显然，这样一组数满足题设要求.

当 t 为偶数时，类似地取 $2t$，2，x 个 1，y 个 -1（x，y 待定），则 $\begin{cases}x+y=4t-2,\\x-y=2t-2.\end{cases}$

解得 $x=3t-2$，$y=t$.

这一组数必满足题设要求.

综上，$4t$（$t\geqslant 2$）型数是迷人的.

下面证明：$4t+2$，$4t+3$ 型数不是迷人的.

若 $4t+2$ 型数是迷人的，设

$4t+2=a_1+a_2+\cdots+a_{4t+2}=a_1a_2\cdots a_{4t+2}$.

易知，a_i 中有且仅有一个偶数，其余 $4t+1$ 个数均为奇数，故 $a_1+a_2+\cdots+a_{4t+2}$ 必为奇数. 矛盾.

因此，$4t+2$ 型数不是迷人的.

若 $4t+3$ 型数是迷人的，设

$4t+3=a_1a_2\cdots a_{4t+3}=a_1+a_2+\cdots+a_{4t+3}$，其中模 4 余 1 的有 x 个，模 4 余 3 的有 $4t+3-x$ 个.

故 $x+3(4t+3-x)\equiv 3 \pmod 4$.

所以，$2x\equiv 2 \pmod 4$.

于是，x 为奇数，$4t+3-x$ 为偶数.

则 $3\equiv 4t+3=a_1a_2\cdots a_{4t+3}\equiv 1^x\times 3^{4t+3-x}\equiv 1 \pmod 4$.

矛盾.

因此，$4t+3$ 型数不是迷人的.

综上所述，全部迷人的数为

$4t+1$，$t\in\mathbf{N}$；$4t$，$t\in\mathbf{N}$，$t\geqslant 2$.

12. 令 $S(n,r)=\dfrac{n+1-2r}{n+1-r}C_n^r$.

(1) $$S(n,r)=\frac{n+1-r}{n+1-r}C_n^r-\frac{r}{n+1-r}C_n^r=C_n^r-\frac{r\cdot n!}{r!\,(n+1-r)(n-r)!}$$

$$=C_n^r-\frac{n!}{(r-1)!\,(n+1-r)!}=C_n^r-C_n^{r-1}.$$

故 $S(n,r)$ 为整数.

(2) $$\sum_{r=0}^{[\frac{n}{2}]}\frac{n+1-2r}{n+1-r}C_n^r=\sum_{r=0}^{[\frac{n}{2}]}S(n,r)=S(n,0)+\sum_{r=1}^{[\frac{n}{2}]}S(n,r)=1+\sum_{r=1}^{[\frac{n}{2}]}(C_n^r-C_n^{r-1})=C_n^{[\frac{n}{2}]}.$$

故只需证 $C_n^{[\frac{n}{2}]}<2^{n-2}$（$n\geqslant 9$）.

下面用数学归纳法并分 n 的奇偶性进行讨论.

(i) 设 $n=2m$ $(m\geqslant 5)$，则

$$C_n^{[\frac{n}{2}]}=\frac{(2m)!}{(m!)^2}.$$

当 $m=5$ 时，$C_{10}^5<2^8$，成立.

设 $m=k$ $(k\geqslant 5)$ 时，命题成立.

当 $m=k+1$ 时，

$$\frac{[2(k+1)]!}{[(k+1)!]^2}=\frac{2(k+1)(2k+1)}{(k+1)^2}\cdot\frac{(2k)!}{(k!)^2}<\frac{2k+1}{k+1}\cdot 2^{2k-1}<2^{2k}.$$

故对任意 m $(m\geqslant 5)$，原命题成立.

(ii) 设 $n=2m+1$ $(m\geqslant 4)$，则

$$C_n^{[\frac{n}{2}]}=C_n^m=\frac{(2m+1)!}{m!\ (m+1)!}.$$

当 $m=4$ 时，易知 $C_9^4<2^7$.

设 $m=k$ $(k\geqslant 4)$ 时，原命题成立.

当 $m=k+1$ 时，

$$\frac{(2k+3)!}{(k+1)!\ (k+2)!}=\frac{(2k+3)(2k+2)}{(k+2)(k+1)}\cdot\frac{(2k+1)!}{k!\ (k+1)!}<\frac{2k+3}{k+2}\times 2^{2k}<2^{2k+1}.$$

故对任意的 m $(m\geqslant 4)$，原命题成立.

综上，对任意的 n $(n\geqslant 9)$，原不等式成立.

13. 先证明一个引理.

引理 题设数列满足

$$x_{2n+1}=x_n+1,\ \frac{1}{x_{2n}}=\frac{1}{x_n}+1.$$

引理的证明：用数学归纳法.

当 $k=1$ 时，$x_1=1$，$x_2=\frac{1}{2}$，$x_3=2$，所以，

$$x_3=2=1+1=x_1+1,$$

$$\frac{1}{x_2}=2=1+1=\frac{1}{x_1}+1.$$

结论成立.

设当 $k=n-1$ 时，有

$$x_{2n-1}=x_{n-1}+1,\ \frac{1}{x_{2n-2}}=\frac{1}{x_{n-1}}+1.$$

结论成立.

当 $k=n$ 时，有

$$x_{2n}=\frac{1}{1+2f(2n)-x_{2n-1}}=\frac{1}{3+2f(n)-\cfrac{1}{1+2f(2n-1)-x_{2n-2}}}\text{[因为 } f(2n)=1+f(n)\text{]}$$

$$=\frac{1}{3+2f(n)-\frac{1}{1-x_{2n-2}}}\text{[因为 }f(2n-1)=0\text{]}$$

$$=\frac{1}{3+2f(n)-\frac{1}{1-\frac{1}{\frac{1}{x_{n-1}}+1}}}=\frac{1}{3+2f(n)-(x_{n-1}+1)}.$$

则$\frac{1}{x_{2n}}-1=1+2f(n)-x_{n-1}=\frac{1}{x_n}$.

所以，$x_{2n}=\frac{x_n}{x_n+1}$.

$x_{2n+1}=\frac{1}{1+2f(2n+1)-x_{2n}}=x_n+1$.

结论成立.

故引理得证.

下面证明原题.

先证明$\frac{p}{q}$[$(p,q)=1$，$p\geqslant0$，$q>0$] 在数列中.

由 $x_{2n+1}=x_n+1$，$x_0=0$，则只须证$\frac{p}{q}$[$(p,q)=1$，$0<p<q$] 在数列中.

对 q 用数学归纳法.

当 $q=2$ 时，有 $x_2=\frac{1}{2}$在数列中.

设 $q\leqslant k-1$ 时，$\frac{p}{q}$在数列中.

当 $q=k$ 时，由归纳假设$\frac{p}{q-p}=x_t$ 在数列中，故 $x_{2t}=\frac{x_t}{x_t+1}=\frac{p}{q}$在数列中.

再证每个非负有理数仅出现一次.

若不然，设 $x_t=x_s$，且 t 最小，$t<s$.

(1) 若 s，t 同奇，则 $x_{\frac{t-1}{2}}=x_t-1=x_s-1=x_{\frac{s-1}{2}}$，所以，$\frac{t-1}{2}\geqslant t$，即 $t\leqslant-1$，矛盾.

(2) 若 s，t 同偶，同理可推得矛盾.

(3) 若 s，t 一奇一偶，但 $x_{奇}\geqslant1$，$x_{偶}<1$，则 $x_t\neq x_s$，矛盾.

14. 这里需要用到 Euler 的一个结论：

n 为偶完全数$\Leftrightarrow$存在素数 p，使得 2^p-1 为素数，且 $n=2^{p-1}(2^p-1)$.

下面以此来解本题.

情形一：n 为奇数，则 $n-1$ 为偶完全数，于是，可写 $n-1=2^{p-1}(2^p-1)$，其中 p 与 2^p-1 都为素数，这时

$$\frac{n(n+1)}{2}=\frac{1}{2}(2^{p-1}(2^p-1)+1)(2^{p-1}(2^p-1)+2)=(2^{p-1}(2^p-1)+1)(2^{p-2}(2^p-1)+1).$$

当 $p=2$ 时，$n=7$，$\frac{n(n+1)}{2}=28$，此时 $n-1$ 与 $\frac{n(n+1)}{2}$ 都是完全数.

当 $p\geqslant3$ 时，记 $N=\frac{n(n+1)}{2}$，则 N 为奇数，且

$$\frac{n+1}{2}=4^{p-1}-2^{p-2}+1=(3+1)^{p-1}-(3-1)^{p-2}+1,$$

用二项式定理可知 $\equiv3\times(p-1)-(p-2)\times3+1+1+1\equiv6 \pmod 9$.

从而 $3\mid N$，但 $3^2\nmid N$，可设 $N=3k$，$3\nmid k$，此时，$\sigma(N)=\sigma(3)\sigma(k)=4\sigma(k)$，但是 $2N\equiv2 \pmod 4$，故 $\sigma(N)\neq2N$，从而此时 $\frac{n(n+1)}{2}$ 不是完全数.

情形二：n 为偶数，如果 $4\mid n$，则 $n-1\equiv-1 \pmod 4$ $\Rightarrow n-1$ 不是完全平方数，此时对任意 $d\mid n-1$，由 $d\times\frac{n-1}{d}=n-1\equiv-1 \pmod 4$，可知 d 与 $\frac{n-1}{d}$ 中一个 mod 4 余 -1，另一个 mod 4 余 1，导致 $d+\frac{n-1}{d}\equiv0 \pmod 4$，从而 $4\mid\sigma(n-1)$，但 $2(n-1)\equiv2 \pmod 4$，故 $n-1$ 不是完全数.

所以，$4\nmid n$，于是，可设 $n=4k+2$，此时 $N=\frac{n(n+1)}{2}=(2k+1)(4k+3)$ 为奇数. 由于 $(2k+1, 4k+3)=1$，故 $\sigma(N)=\sigma(2k+1)\sigma(4k+3)$.

同上可知 $4\mid\sigma(4k+3)$，故若 $\sigma(N)=2N$，则 $4\mid2N\Rightarrow2\mid N$，这是一个矛盾.

综上可知，满足条件的 n 只有一个，即 $n=7$.

第五章 素数、合数及威尔逊定理

习题 A

1. 已知数可化为

$$\begin{aligned}4^{545}+545^4&=(2^{545})^2+2\cdot2^{545}\cdot545^2+(545)^4-2\cdot2^{545}\cdot545^2\\&=(2^{545}+545^2)^2-2^{546}\cdot545^2=(2^{545}+545^2)^2-(2^{273}\cdot545)^2\\&=(2^{545}+545^2+2^{273}\cdot545)(2^{545}+545^2-2^{273}\cdot545),\end{aligned}$$

因此该数是合数.

2. $1\underbrace{00\cdots0}_{161个}1=10^{1962}+1=(10^{654})^3+1=(10^{654}+1)(10^{1308}-10^{654}+1)$，

因而 $1\underbrace{00\cdots0}_{161个}1$ 是合数.

3. 由于 $2^{1974}+2^{1000}=2^{1000}(2^{974}+1)$，则

数 $A=1\underbrace{00\cdots0}_{2^{1974}+2^{1000}-1个0}1=1\underbrace{00\cdots00}_{2^{1974}+2^{1000}个0}+1=(10^{2^{1000}})^{2^{974}+1}+1$.

记 $10^{2^{1000}}=a$，$2^{974}+1=n$，则 n 是奇数.

于是 $A=a^n+1$ 能被 $a+1>1$ 整除，从而 A 是合数.

4. $\underbrace{11\cdots1}_{n个}2\underbrace{11\cdots1}_{n个}=\underbrace{11\cdots11}_{n+1个}\underbrace{00\cdots0}_{n个}+\underbrace{11\cdots11}_{n+1个}=\underbrace{11\cdots11}_{n+1个}(1\underbrace{00\cdots0}_{n个}+1)-(\underbrace{11\cdots11}_{n+1个})\cdot(10^n+1)$，

所以是合数.

5. 注意到 $p^3+2p^2+p=p(p+1)^2$.

由 p 与 $p+1$ 互素，可以证明：p^3+2p^2+p 的因数为 p 的因数与 $(p+1)^2$ 的因数之积.

因为 p 只能有两个因数，所以 $(p+1)^2$ 有 21 个因数.

又 $21=3\cdot7$，为使 p 最小，取 $(p+1)^2=2^6\cdot3^2$，即 $p+1=24$，故 $p=23$.

6. 当 28 与 56 被 3 除时，余数分别是 1 和 2，于是，素数 p 被 3 除时，余数既不是 1，也不是 2，否则，数 $p+28$ 或 $p+56$ 中将有一个能被 3 整除. 但能被 3 整除的素数只有一个，就是素数 3 本身，这时，$p+28=31$，$p+56=59$，也都是素数，这就是所要求的.

7. 定义数列 $\{a_n\}$ 满足 $a_n=2^{2^n}+1$，则

$a_0a_1a_2\cdots a_{n-1}=a_n-2$，且当 $n\neq m$ 时，$\gcd(a_n,a_m)=1$.

对所有满足 $n\geqslant a$ 的正整数 n，记 p_n 为 a_n 的任一素因数，则当 $n\neq m$ 时，$p_n\neq p_m$.

假设对某些正奇数 b，$2^{2^n b}-1$ 能被 p_n 整除.

由 $a^{2^n b}\equiv1\pmod{p_n}$，$2^{2^{n+1}}\equiv1\pmod{p_n}$，得

$2^{2^n}\equiv1\pmod{p_n}$.

这与 $2^{2^n}\equiv-1\pmod{p_n}$ 矛盾.

因此，对所有满足 $n\geqslant a$ 的正整数 n，$p_n\notin S_n$.

8. 若 $p\equiv1\pmod 3$，则

$p+14\equiv15\equiv0\pmod 3$.

此时，$p+14$ 不是素数.

若 $p\equiv2\pmod 3$，则

$p+10\equiv12\equiv0\pmod 3$.

此时，$p+10$ 不是素数.

所以 $p\equiv0\pmod 3$.

又由 p 是素数，则 $p=3$.

此时 $p+10=13$，$p+14=17$ 都是素数.

所以本题只有唯一解：$p=3$.

9. 设三个素数为 p，q，r，则

$p\cdot q\cdot r=5(p+q+r)$.

于是，p，q，r 中必有一个等于 5. 不妨设 $r=5$，则

$5pq=5(p+q+5)$，

$pq=p+q+5$，

$(p-1)(q-1)=6$.

由 $p>1$，$q>1$ 可知

$\begin{cases}p-1=2,\\q-1=3,\end{cases}\begin{cases}p-1=3,\\q-1=2,\end{cases}\begin{cases}p-1=1,\\q-1=6,\end{cases}\begin{cases}p-1=6,\\q-1=1.\end{cases}$

由于 $q=4$ 或 $p=4$ 不是素数，所以只有 $p=2$，$q=7$，或 $p=7$，$q=2$，于是所求三素数为 2，5，7.

10. $n=C_{200}^{100}=\dfrac{200\cdot199\cdot198\cdot\cdots\cdot102\cdot101}{100!}=2^{50}\cdot\dfrac{199\cdot197\cdot195\cdot\cdots\cdot103\cdot101}{50!}$，

这是一个整数，且分子中 $199\cdot197\cdot195\cdot\cdots\cdot103\cdot101$ 是三位奇数之积，于是所求的两位数的素因子只能从三位奇合数中寻找.

由于小于 200 的合数一定含有小于 $\sqrt{200}$ 的素数为因子，因此在 101 到 199 之间的奇合数的素因子一定含有 3，5，7，11，13 中的一个.

由于 $\left[\dfrac{199}{3}\right]=66$，于是所求的最大的两位素因子一定小于 66，而小于 66 的最大的素数为 61，且 $61\cdot3=183$ 恰为 C_{200}^{100} 中的一个因子，于是所求的最大素因子为 61.

11. 设整数 x 使

$q=x^3(p-x)$， ①

于是 $x\mid q$.

因为 q 是素数，因此只能有

$x=\pm1$，$x=\pm q$.

当 $x=\pm q$ 时，由①有

$q^2\mid 1$，这是不可能的（因为 q 是素数）.

当 $x=-1$ 时，有

$p+q+1=0$，这也不可能.

当 $x=1$ 时，由①式得

$p=q+1$.

因为 p 和 q 都是素数，则 $p=3$，$q=2$.

习题 B

1. 显然 $p<19$.

如果 p 是奇数，则 p^p+1 能被 2 整除，于是仅当 $p=1$ 时，$p^p+1=2$ 是素数.

如果 p 有奇数因子，设 $p=mk$，其中 m 是奇数，则

$p^p+1=p^{mk}+1=(p^k)^m+1$，此时 $p^k+1\mid p^p+1$.

因而 p^p+1 不是素数.

于是 p 仅可能是小于 19 的偶数，且只有偶数因子，即

$p=2$，4，8，16.

若 $p=16$，则

$16^{16}=2^{64}=(2^{10})^6\cdot16>1000^6\cdot16=16\cdot10^{18}$，

因此 $16^{16}+1$ 多于 19 位数.

若 $p=8$，则

$8^8+1=2^{24}+1=(2^8)^3+1=(2^8+1)(2^{16}-2^8+1)$是合数.

若 $p=4$，则

$4^4+1=257$ 是素数.

若 $p=2$，则

$2^2+1=5$ 是素数.

于是所求的素数为 2，5，257.

2. 若 $2p+1$ 是自然数的方幂，即 $2p+1=m^n$，则 m 为奇数.

设 $m=2k+1$，则

$2p+1=(2k+1)^n$.

从而 $2p=2k\cdot A$，即 $p=k\cdot A$，其中 p 是素数，A 是大于 1 的整数.

由 p 是素数可知，$k=1$，因而 $m=3$，即

$2p+1=3^n$. ①

由 $p\leqslant 1000$，则 $3^n\leqslant 2001$.

而不超过 2001 的 3 的幂仅有

3，3^2，3^3，3^4，3^5，3^6，

代入①式逐个计算可得，仅有 $2p+1=3^3$ 使 p 为素数，此时 $p=13$.

即符合题目要求的素数仅有一个，$p=13$.

3. 设这 8 个素数为 x_1，x_2，…，x_8.

设 $S=x_1^2+x_2^2+\cdots+x_8^2$，$P=x_1x_2\cdots x_8$.

由题意有

$4P-S=992$. ①

首先，所有的 x_i 不可能都是奇数.

由于奇数的平方被 8 除的余数为 1，则

$S\equiv 0 \pmod 8$.

又 $4P\equiv 4 \pmod 8$，

$992\equiv 0 \pmod 8$.

则①式不可能成立.

其次，所有的 x_i 不可能有一部分是奇素数，另一部分是 2.

设有 k 个奇素数，$8-k$ 个 $2(1\leqslant k\leqslant 7)$，由于

$4P\equiv 0 \pmod 8$，

$S\equiv k+4(8-k)\equiv 32-3k \pmod 8$，

$992\equiv 0 \pmod 8$，

于是①式也不可能成立.

由以上，所有的 $x_i(i=1,2,\cdots,8)$ 都是 2.

经验证，$x_1=x_2=\cdots=x_8=2$ 符合要求.

4. 因为 p_i 是不小于 5 的素数，则 p_i 仅可表示为 $6k\pm1$ 型（k 为自然数），于是

$p_i^2-1=36k^2\pm12k=12k(3k\pm1)$.

由于 k 和 $3k\pm1$ 的奇偶性不同，所以 $k(3k\pm1)$ 是偶数，于是 p_i^2-1 能被 24 整除. 从而

$p_1^2+p_2^2+\cdots+p_{24}^2-24$

能被 24 整除，即 $p_1^2+p_2^2+\cdots+p_{24}^2$ 能被 24 整除.

5. $p^q+q^p=(p^p+q^p)+(p^q-p^p)=(p^p+q^p)+(p^{p+2}-p^p)$，

因为 p 和 q 都是素数，且 $q=p+2$，则 p 和 q 都是奇数.

由 p 是奇数，则

$p+q\mid p^p+q^p$.

又 $p^{p+2}-p^p=p^p(p-1)(p+1)$，

由于 $p-1$ 是偶数，则

$2(p+1)\mid p^p(p-1)(p+1)$.

又 $2(p+1)=2p+2=p+q$，

于是 $p+q\mid p^{p+2}-p^p$.

因此 $p+q\mid p^q+q^p$.

6. 满足条件的整数组 $(a,b,c)=(1,-1,p)$. 我们证明它是唯一的解.

由 $b^2-4ac=1-4p$， ①

可得 b 是满足 $b^2\equiv1 \pmod 4$ 的整数，因而 b 是奇数.

记 $|b|=2x-1$，则由①式得

$(2x-1)^2-4ac=1-4p$，即 $x^2-x+p=ac$.

若 $0\leqslant x<p$，由题设可知 ac 是素数.

则由 $0<a\leqslant c$ 得 $a=1$.

再由 $-a\leqslant b<a$ 及 b 是奇数可得 $b=-1$.

又由 $1-4p=b^2-4ac=1-4c$，可得 $c=p$.

下面只要证明 $0\leqslant x<p$ 即可.

由 $|b|=2x-1$ 可得

$x=\frac{|b|+1}{2}\geqslant0$.

由 $|b|\leqslant a\leqslant c$，$b^2-4ac=1-4p$ 及 $p\geqslant2$，则

$3a^2=4a^2-a^2\leqslant4ac-b^2=4p-1$，

$|b|\leqslant a\leqslant\sqrt{\frac{4p-1}{3}}$，

$x=\frac{|b|+1}{2}<\sqrt{\frac{p}{3}}+\frac{1}{2}<p$.

于是 $0\leqslant x<p$.

由以上，唯一性得证.

7. 因为 p，q 是正素数，所以原方程不可能有正数根。

又因为已知方程的 x^2 的系数为 1，所以若方程有有理根，则只能是整数根，且必为 q^3 的约数.

因此，若原方程有有理根，则只能取以下各数：-1，$-q$，$-q^2$，$-q^3$.

若方程的两根为 $-q$，$-q^2$，则由韦达定理

$p^2=q+q^2=q(q+1)\geqslant 6$.

此时 p^2 为偶数，且 $p^2\neq 4$，所以 p 必为合数，与 p 是素数矛盾.

因而 $-q$，$-q^2$ 不是原方程的根.

若方程有有理根，只能是 -1 和 $-q^3$，这时有

$p^2=1+q^3$，

显然，q 不能为奇素数，否则 p^2 为大于 4 的偶数，因而 p 是合数，于是 q 为偶素数，即 $q=2$，从而 $p=3$.

所以当且仅当 $p=3$，$q=2$ 时，原方程 $x^2+p^2x+q^3=0$ 即 $x^2+9x+8=0$ 有有理根，$x_1=-1$，$x_2=-8$.

8. 设 $n=3^kr$，其中 k 是非负整数，且 $3\nmid r$.

我们证明，此时 $p=1+2^n+4^n$ 被 $q=1+2^{3^k}+4^{3^k}$ 整除，从而 p 不是素数.

(1) $r=3s+1$ 时，s 是非负整数，则

$p-q=(2^n-2^{3^k})+(4^n-4^{3^k})=2^{3^k}(2^{3^k\cdot 3s}-1)+4^{3^k}(2^{3^k\cdot 6s}-1)\equiv 0(\mathrm{mod}\ (2^{3^k\cdot 3}-1))$.

因为 $2^{3^k\cdot 3}-1=(2^{3^k}-1)(1+2^{3^k}+4^{3^k})=(2^{3^k}-1)q$，

所以 $q\mid p-q$，于是 $q\mid p$.

(2) $r=3s+2$ 时，s 是非负整数，则

$p-q=(4^n-2^{3^k})+(2^n-4^{3^k})=2^{3^k}[2^{3^k3(2s+1)}-1]+2^{2\cdot 3^k}(2^{3^k\cdot 3s}-1)\equiv 0(\mathrm{mod}\ (2^{3^k\cdot 3}-1))$.

同 (1)，仍有 $q\mid p$.

于是 $n=3^kr$，$3\nmid r$ 时，p 为合数，从而当 $p=1+2^n+4^n$ 是素数时，$n=3^k$.

9. 由于 $m^3-m=m(m-1)(m+1)\equiv 0(\mathrm{mod}\ 3)$，所以

$q_i=(q_{i-1}-1)^3+3\equiv(q_{i-1}-1)^3\equiv q_{i-1}-1(\mathrm{mod}\ 3)$.

因而 q_1，q_2，q_3 中必有一个能被 3 整除，这个数应当是 3 的幂.

若 $3\mid(q-1)^3+3$，则 $3\mid(q-1)^3$，于是 $3\mid q-1$.

故 $3^3\mid(q-1)^3$.

而 $3\mid(q-1)^3+3$，

于是只有在 $q_i=1$ 时，$(q_i-1)^3+3$ 才是 3 的幂，这时必须 $i=0$.

但 $q_0=1$ 时推出

$q_1=3$，$q_2=11$，$q_3=1003=17\cdot 59$.

所以 n 的最大值是 2.

10. 集合 A 中的元素个数的最大值为 p^{n-2}.

易知集合 A 中的任意两个不同序列的前 $n-2$ 个分量不全相同（否则这两个序列至多有 2 个分量不同，矛盾），每个分量均有 p 种取值，因此，

$|A|\leqslant p^{n-2}$.

另一方面，令 A 中的某一序列 $(x_1, x_2, \cdots, x_n)$ 中的前 $n-2$ 个分量取遍 p^{n-2} 种不同的值，并取

$$x_{n-1}\equiv\sum_{i=1}^{n-2}x_i \pmod p, x_n\equiv\sum_{i=1}^{n-2}ix_i \pmod p.$$

这样就得到一个 p^{n-2} 元的集合 A.

下面证明该集合 A 符合要求.

对于 A 中的任意两个不同的序列：$X=(x_1,x_2,\cdots,x_n)$ 和 $Y=(y_1,y_2,\cdots,y_n)$，有

$(x_1,x_2,\cdots,x_{n-2})\neq(y_1,y_2,\cdots,y_{n-2})$.

若 $(x_1,x_2,\cdots,x_{n-2})$ 与 $(y_1,y_2,\cdots,y_{n-2})$ 至少有 3 个对应的分量不同，则 X 与 Y 至少有 3 个对应的分量不同.

若 $(x_1,x_2,\cdots,x_{n-2})$ 与 $(y_1,y_2,\cdots,y_{n-2})$ 恰有 2 个对应的分量不同，即存在 k，l $(1\leqslant k<l\leqslant n-2)$，使得

$x_k\neq y_k$，$x_l\neq y_l$.

假设此时 $x_{n-1}=y_{n-1}$，$x_n=y_n$，则

$$x_k+x_l\equiv y_k+y_l \pmod p, \quad ①$$

$$kx_k+lx_l\equiv ky_k+ly_l \pmod p. \quad ②$$

②$-k\times$①得

$(l-k)x_l=(l-k)y_l \pmod p$.

由 $1\leqslant l-k<p$，即 $(p, l-k)=1$，知

$x_l\equiv y_l \pmod p$.

故 $x_l=y_l$，矛盾.

因此，X 和 Y 至少有 3 个对应的分量不同.

若 $(x_1,x_2,\cdots,x_{n-2})$ 与 $(y_1,y_2,\cdots,y_{n-2})$ 只有 1 个对应的分量不同，即存在 k $(1\leqslant k\leqslant n-2)$，使得

$x_k\neq y_k$.

于是，由 $1\leqslant|y_k-x_k|<p(1\leqslant k<p)$，得

$y_{n-1}-x_{n-1}\equiv y_k-x_k\not\equiv0 \pmod p$,

$y_n-x_n\equiv k(y_k-x_k)\not\equiv0 \pmod p$.

因此，$y_{n-1}\neq x_{n-1}$，$y_n\neq x_n$，此时，X 和 Y 亦有 3 个对应的分量不同.

综上所述，所求集合 A 中的元素个数的最大值为 p^{n-2}.

11. 据条件，

$$(a+1)(c+1)=(b+1)^2. \quad ①$$

设 $a+1=n^2x$，$c+1=m^2y$，其中 x，y 不含大于 1 的平方因子，则必有 $x=y$，这是由于，据①，

$$(mn)^2xy=(b+1)^2, \quad ②$$

则 $mn\mid(b+1)$，设 $b+1=mn\cdot w$，于是②化为，

$$xy=w^2. \tag{③}$$

若 $w>1$，则有素数 $p_1|w$，即 $p_1^2|w^2$，因 x,y 皆不含大于 1 的平方因子，因此 $p_1|x$，$p_1|y$. 设

$$x=p_1x_1，\ y=p_1y_1，\ w=p_1w_1，$$

则③化为，

$$x_1y_1=w_1^2； \tag{④}$$

若仍有 $w_1>1$，则又有素数 $p_2|w_1$，即 $p_2^2|w_1^2$，因 x_1,y_1 皆不含大于 1 的平方因子，则 $p_2|x_1$，$p_2|y_1$. 设

$$x_1=p_2x_2，\ y_1=p_2y_2，\ w_1=p_2w_2，$$

则④化为，$x_2y_2=w_2^2$，……，如此下去，因③式中 w 的素因子个数有限，故有 r，使 $w_r=1$，而从 $x_ry_r=w_r^2$ 得，$x_r=y_r=1$，从而 $x=p_1p_2\cdots p_r=y$，改记 $x=y=k$，则有

$$\begin{cases}a=kn^2-1,\\ b=kmn-1,\\ c=km^2-1,\end{cases} \tag{⑤}$$

其中 $1\leqslant n<m$，$a<b<c<100$， ⑥

k 无大于 1 的平方因子，并且 $k\neq1$，否则若 $k=1$，则 $c=m^2-1$，因 c 大于第三个素数 5，即 $c=m^2-1>5$，$m\geqslant3$，得

$$c=m^2-1=(m-1)(m+1)$$

为合数，矛盾. 因此 k 或为素数，或为若干个互异素数之乘积（即 k 大于 1，且无大于 1 的平方因子）. 我们将其简称为"k 具有性质 p".

(1) 据⑥，$m\geqslant2$. 当 $m=2$，则 $n=1$，有 $\begin{cases}a=k-1,\\ b=2k-1,\\ c=4k-1,\end{cases}$ 因 $c<100$，得 $k<25$.

若 $k\equiv1 \pmod 3$，则 $3|c$ 且 $c>3$，得 c 为合数.

若 $k\equiv2 \pmod 3$，在 k 为偶数时，具有性质 p 的 k 有 2，14，分别给出 $a=2-1=1$，$b=2\cdot14-1=27$ 不为素数；k 为奇数时，具有性质 p 的 k 值有 5，11，17，23，分别给出的 $a=k-1$ 皆不为素数.

若 $k\equiv0 \pmod 3$，具有性质 p 的 k 值有 3，6，15，21，当 $k=3$ 时，给出解 $f_1=(a,b,c)=(2,5,11)$；当 $k=6$ 时，给出解 $f_2=(a,b,c)=(5,11,23)$；$k=15$，21 时，分别给出的 $a=k-1$ 皆不为素数.

若 $m=3$，则 $n=2$ 或 1.

在 $m=3$，$n=2$ 时，$\begin{cases}a=4k-1,\\ b=6k-1,\\ c=9k-1,\end{cases}$ 因素数 $c\leqslant97$，得 $k\leqslant10$，具有性质 p 的 k 值有 2，3，5，6，7，10. 在 k 为奇数 3，5，7 时，给出 $c=9k-1$ 皆为合数；在 $k=6$ 时，给出 $b=6k-1=35$ 为合数；$k=10$ 时，给出 $a=4k-1=39$ 为合数；在 $k=2$ 时，给出解 $f_3=(a,b,c)=(7,11,17)$.

在 $m=3$，$n=1$ 时，$\begin{cases}a=k-1,\\ b=3k-1,\\ c=9k-1,\end{cases}$ $k\leqslant10$，具有性质 p 的 k 值有 2，3，5，6，7，10. 在 k 为奇数

3，5，7 时，给出的 $b=3k-1$ 皆为合数；$k=2$ 和 10 时，给出的 $a=k-1$ 不为素数；$k=6$ 时，给出解 $f_4=(a,b,c)=(5,17,53)$.

(2) $m=4$ 时，由 $c=16k-1\leqslant 97$，得 $k\leqslant 6$，具有性质 p 的 k 值有 2，3，5，6.

在 $k=6$ 时，$c=16\cdot 6-1=95$ 为合数.

$k=5$ 时，$\begin{cases}a=5n^2-1,\\ b=20n-1,\end{cases}$因 $n<m=4$，则 n 可取 1，2，3，分别得到 a，b 至少一个不为素数.

$k=3$ 时，$c=48-1=47$，$\begin{cases}a=3n^2-1,\\ b=12n-1,\end{cases}$因 $n<m=4$，在 $n=3$ 时给出的 a，b 为合数.

$n=2$ 时给出解 $f_5=(a,b,c)=(11,23,47)$；

$n=1$ 时给出解 $f_6=(a,b,c)=(2,11,47)$.

$k=2$ 时，$c=16k-1=31$，$\begin{cases}a=2n^2-1,\\ b=8n-1,\end{cases}$ $n<m=4$，只有在 $n=3$ 时给出解 $f_7=(a,b,c)=(17,23,31)$.

(3) $m=5$ 时，$c=25k-1\leqslant 97$，具有性质 p 的 k 值有 2，3，分别给出 $c=25k-1$ 为合数.

(4) $m=6$ 时，$c=36k-1\leqslant 97$，具有性质 p 的 k 值只有 2，得 $c=2\cdot 36-1=71$，这时 $\begin{cases}a=2n^2-1,\\ b=12n-1,\end{cases}$ $n<m=6$，只有在 $n=2$ 时给出解 $f_8=(a,b,c)=(7,23,71)$；在 $n=4$ 时给出解 $f_9=(a,b,c)=(31,47,71)$.

(5) $m=7$ 时，$c=49k-1\leqslant 97$，具有性质 p 的 k 值只有 2，得 $c=2\cdot 49-1=97$，而 $n<m=7$，$\begin{cases}a=2n^2-1,\\ b=14n-1,\end{cases}$只有在 $n=3$ 时给出解 $f_{10}=(a,b,c)=(17,41,97)$；在 $n=6$ 时给出解 $f_{11}=(a,b,c)=(71,83,97)$.

(6) $m\geqslant 8$ 时，$c=64k-1\leqslant 97$，具有性质 p 的 k 值不存在.

因此，满足条件的解共有 11 组，即为上述的 f_1，f_2，…，f_{11}.

第六章　素因数分解

1. 设 d_1 是 n 的一个正约数，则 $d_2=\frac{n}{d_1}$ 也是 n 的一个正约数，于是

$\min\{d_1, d_2\}\leqslant\sqrt{n}$.

把 n 的所有正约数两两配对（当 n 为完全平方数时，$\sqrt{n}$除外），从而正约数的总个数不超过 $\sqrt{n}+\sqrt{n}=2\sqrt{n}$.

2. 因为当且仅当 n 是平方数时，$N(n)$是奇数.

又因为　$44^2<1989<45^2$，

所以 1，2，…，1989 中有 44 个完全平方数，即在数 $N_{(1)}$，$N_{(2)}$，…，$N_{(1989)}$ 中有 44 个奇数，其余为偶数，

于是 $N_{(1)}+N_{(2)}+\cdots+N_{(1989)}$ 是偶数.

3. 设 $q=2^p-1$ 为素数.

数 $n=2^{p-1}q$ 的一切小于它本身的约数为

$1, 2, 2^2, \cdots, 2^{p-2}, 2^{p-1}$;

$q, 2q, 2^2q, \cdots, 2^{p-2}q$.

由于

$1+2+2^2+\cdots+2^{p-2}+2^{p-1}=2^p-1=q$,

$q+2q+2^2q+\cdots+2^{p-2}q=(2^{p-1}-1)q$,

则 n 的一切小于它本身的约数之和为

$2^p-1+(2^{p-1}-1)(2^p-1)=2^{p-1}(2^p-1)=n$.

4. 由条件(1),设 $n=75k(k\in\mathbf{N})$.

因为 $75=5^2\cdot 3$, 所以 $n=5^2\cdot 3k$.

又设 $n=5^s\cdot 3^t p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}$, 其中 p_i $(i=1, 2, \cdots, m)$ 为素数, α_i 为非负整数.

由条件 (2), n 的素因数分解式中, 素数的指数应满足

$(s+1)\cdot(t+1)\cdot(\alpha_1+1)\cdot\cdots\cdot(\alpha_m+1)=75$.

因而其指数应为 2, 4, 4 或 2, 24, 或 4, 14.

为使 n 最小, 显然为

$n=5^2\cdot 3^4\cdot 2^4$.

于是 $k=\frac{n}{75}=3^3\cdot 2^4=432$.

5. 由题意 $24\mid n+1$ 等价于 $\begin{cases} n\equiv -1 \pmod 3, \\ n\equiv -1 \pmod 8. \end{cases}$

设 d 是 n 的一个约数, 即 $d\mid n$, 则有

$d\equiv 1$ 或 $2 \pmod 3$,

$d\equiv 1, 3, 5$ 或 $7 \pmod 8$.

再由 $d\cdot\frac{n}{d}=n\equiv -1 \pmod 3$ 或 $\pmod 8$ 可知, 仅有下列几种可能:

$d\equiv 1, \frac{n}{d}\equiv 2 \pmod 3$,

$d\equiv 1, \frac{n}{d}\equiv 7 \pmod 8$,

$d\equiv 3, \frac{n}{d}\equiv 5 \pmod 8$.

反之, 以上由三个同余式也可得

$n\equiv -1 \pmod 3$ 或 $\pmod 8$.

于是有 $d+\frac{n}{d}\equiv 0 \pmod 3$, $d+\frac{n}{d}\equiv 0 \pmod 8$, 即

$d+\frac{n}{d}\equiv 0 \pmod{24}$.

因而对于 $n \equiv 1 \pmod 3$，n 不是完全平方数，所以 $d \neq \frac{n}{d}$，所以 n 的约数两两互异，即 n 的全体约数之和一定能被 24 整除.

6. 如果对于某个正整数 n，有 $\tau(an)=n$，则 $a=\frac{an}{\tau(an)}$，于是，关于正整数 k 的方程 $\frac{k}{\tau(k)}=a$ 有解. 因此，只须证明：

若素数 $p \geqslant 5$，则方程 $\frac{k}{\tau(k)}=p^{p-1}$ 没有正整数解.

设 n 在区间 $[1, \sqrt{n}]$ 内有 k 个因数，则在区间 $(\sqrt{n}, n]$ 内至多有 k 个因数. 事实上，如果 d 是一个比 $\sqrt{n}$ 大的 n 的因数，则 $\frac{n}{d}$ 就是一个比 $\sqrt{n}$ 小的 n 的因数. 故 $\tau(n) \leqslant 2k \leqslant 2\sqrt{n}$.

假设对于某个素数 $p \geqslant 5$，方程 $\frac{k}{\tau(k)}=p^{p-1}$ 有正整数解 k，则 k 能被 p^{p-1} 整除. 设 $k=p^{\alpha}s$，其中 $\alpha \geqslant p-1$，p 不能整除 s. 于是，有

$$\frac{p^{\alpha}s}{(\alpha+1)\tau(s)}=p^{p-1}.$$

若 $\alpha=p-1$，则 $s=p\tau(s)$.

所以，p 整除 s，矛盾.

若 $\alpha \geqslant p+1$，则

$$\frac{p^{p-1}(\alpha+1)}{p^{\alpha}}=\frac{s}{\tau(s)} \geqslant \frac{s}{2\sqrt{s}}=\frac{\sqrt{s}}{2}.$$

因为对于所有 $p \geqslant 5$，$\alpha \geqslant p+1$，有 $2(\alpha+1)<p^{\alpha-p+1}$（对 α 用数学归纳法容易证明），所以，可得 $s<1$，矛盾.

若 $\alpha=p$，则 $ps=(p+1)\tau(s)$.

特别地，p 整除 $\tau(s)$，所以，

$$p \leqslant \tau(s) \leqslant 2\sqrt{s}.$$

于是，$\sqrt{s}=\frac{s}{\sqrt{s}} \leqslant \frac{2s}{\tau(s)}=\frac{2(p+1)}{p}$.

从而，$p \leqslant 2\sqrt{s} \leqslant \frac{4(p+1)}{p}$.

对于 $p \geqslant 5$ 而言，这是不可能的.

7. 先证明一个引理.

引理　设 $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m$ 是两组非零整数. 如果对任意大于 1 的正整数 k，都有 $x_1, x_2, \cdots, x_n$ 中能被 k 整除的数的个数不多于 $y_1, y_2, \cdots, y_m$ 中能被 k 整除的数的个数，则

$$x_1x_2\cdots x_n \mid y_1y_2\cdots y_m.$$

引理的证明：设 $f(k)$ 表示 $x_1, x_2, \cdots, x_n$ 中能被 k 整除的数的个数，$g(k)$ 表示 $y_1, y_2, \cdots, y_m$ 中能被 k 整除的数的个数. 对素数 p 和非零整数 x，定义 $V_p(x)$ 为 $|x|$ 的素因数分解式中 p 的幂次.

对任意的素数 p，

$$V_p(x_1x_2\cdots x_n)=\sum_{i=1}^{n}V_p(x_i)=\sum_{i=1}^{n}|\{k|k\in\mathbf{Z}_+,p^k|x_i\}|=|\{(i,k)|i,k\in\mathbf{Z}_+,p^k|x_i\}|=$$

$$\sum_{k=1}^{\infty}|\{i|i\in\mathbf{Z}_+,p^k|x_i\}|=\sum_{k=1}^{\infty}f(p^k).$$

同理，$V_p(y_1y_2\cdots y_m)=\sum\limits_{k=1}^{\infty}g(p^k)$.

而 $f(p^k)\leqslant g(p^k)$，故

$V_p(x_1x_2\cdots x_n)\leqslant V_p(y_1y_2\cdots y_m)$.

又因为 p 可取任意素数，所以，

$x_1x_2\cdots x_n\mid y_1y_2\cdots y_m$.

下面证明原理.

若 a_1，a_2，…，a_n 中有两个数相等，则

$$\prod_{1\leqslant i<j\leqslant n}(a_j-a_i)=0.$$

故 $\prod\limits_{1\leqslant i<j\leqslant n}(j-i)\mid\prod\limits_{1\leqslant i<j\leqslant n}(a_j-a_i)$.

若 a_1，a_2，…，a_n 两两不等，下面证明，对任意正整数 k，$(j-i)$（$1\leqslant i<j\leqslant n$）这 C_n^2 个数中能被 k 整除的数的个数不多于 $(a_j-a_i)(1\leqslant i<j\leqslant n)$ 这 C_n^2 个数中能被 k 整除的数的个数.

对 n 用数学归纳法.

当 $n=2$ 时，命题显然成立.

假设命题对 $n-1$ 成立，证明命题对 n 也成立.

若 $k\geqslant n$，$(j-i)(1\leqslant i<j\leqslant n)$ 这 C_n^2 个数都不能被 k 整除，所以，命题成立.

若 $k<n$，由抽屉原理，在 a_1，a_2，…，a_n 这 n 个数中一定存在 $\left[\frac{n-1}{k}\right]+1$ 个数模 k 的余数相同，不妨设其中一个是 a_n. 于是，(a_n-a_i)（$1\leqslant i<n$）这 $n-1$ 个数中至少有 $\left[\frac{n-1}{k}\right]$ 个能被 k 整除，而 $(n-i)(1\leqslant i<n)$ 这 $n-1$ 个数中恰有 $\left[\frac{n-1}{k}\right]$ 个能被 k 整除.

由归纳假设，$(a_j-a_i)(1\leqslant i<j\leqslant n-1)$ 这 C_{n-1}^2 个数中能被 k 整除的数的个数不少于 $(j-i)(1\leqslant i<j\leqslant n-1)$ 这 C_{n-1}^2 个数中能被 k 整除的数的个数.

所以，$(a_j-a_i)(1\leqslant i<j\leqslant n)$ 这 C_n^2 个数中能被 k 整除的数的个数不少于 $(j-i)(1\leqslant i<j\leqslant n)$ 这 C_n^2 个数中能被 k 整除的数的个数.

因此，命题对 n 也成立.

由引理得：$\prod\limits_{1\leqslant i<j\leqslant n}(j-i)\mid\prod\limits_{1\leqslant i<j\leqslant n}(a_j-a_i)$.

8. 如果 $x_1=a$，则

$$x_2=\left(\frac{1}{2004}+\frac{1}{1}\right)a^2-\frac{1}{2004}+1=\frac{2005a^2+2003}{2004}=a^2+1+\frac{a^2-1}{2004}.$$

因为数列的所有项都是整数，所以，x_2 一定是整数，故 a^2-1 一定能被 $2004=2^2\times3\times167$ 整除.

又因为 a^2-1 能被 4 整除，所以，a^2 一定是奇数，a 也一定是奇数.

设 $a=2b+1$，则

$a^2-1=(a-1)(a+1)=2b(2b+2)=4b(b+1)$.

易知 $b(b+1)$一定能被素数 167 整除.

如果 $b>0$，这就意味着或 b 或 $b+1$ 能被 167 整除，且 $b\geqslant 167$，因此，$a\geqslant 2\times 167+1=335$.

但由题设 $a=x_1<204$，由此得 $b=0$，$a=x_1=1$.

下面计算数列的前几项.

注意到 $x_1=1$，则

$x_2=\left(\frac{1}{2004}+\frac{1}{1}\right)\times 1^2-\frac{1^3}{2004}+1=2$,

$x_3=\left(\frac{2}{2004}+\frac{1}{2}\right)\times 2^2-\frac{2^3}{2004}+1=3$,

$x_4=\left(\frac{3}{2004}+\frac{1}{3}\right)\times 3^2-\frac{3^3}{2004}+1=4$.

再用数学归纳法证明 $x_n=n$ 对所有的正整数 n 是成立的.

当 $n=1，2，3，4$ 时，$x_n=n$ 成立.

假设对某个整数 $k>3$，$x_k=k$ 成立，于是，有

$x_{k+1}=\left(\frac{k}{2004}+\frac{1}{k}\right)\cdot k^2-\frac{k^3}{2004}+1=k+1$.

所以，对所有的正整数 n，$x_n=n$ 成立.

因此，给定数列就是所有正整数的数列. 显然，此数列包括无数个素数.

9. a 是无理数.

若 a 是有理数，则存在正整数 k_0，T，使得对于任意的正整数 $k>k_0$，有 $a_k=a_{k+T}$.

取正整数 m，使得 $mT>k_0$，且 mT 是一个完全平方数. 即若设 $T=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，则取

$m=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}$,

其中，$\alpha_i+\beta_i(i=1,2,\cdots,s)$是偶数，且 β_i 是一个足够大的正整数.

选一个素数 $p>2007$，且 $p\neq p_i(i=1,2,\cdots,s)$，因为 $pmT-mT$ 是 T 的倍数，所以，

$a_{mT}=a_{pmT}$.

设 $\tau(k)$为 k 的正因数的数目，$f(k)$是大于 2007 的 k 的正因数的数目，则

$f(pmT)=f(mT)+\tau(mT)$.

因为 $\tau(mT)$是奇数，$f(pmT)$和 $f(mT)$的奇偶性相同，矛盾.

第七章 整数的可除性特征

1. 由于$\overline{32※35717※}$能被 72 整除，因而它能被 8 和 9 整除.

若一个数能被 8 整除，则这个数的末三位能被 8 整除，显然末三位是 176，即最后一个※号为 6.

若一个数能被 9 整除，则这个数的各位数码之和能被 9 整除，即

$3+2+※+3+5+7+1+7+6=34+※$,

于是※号为 2.

即所求的两个星号数码一个为 2，一个为 6.

2. B 有获胜策略.

B 可以采取这样的策略：

若 A 上一步选 k，则 B 选 $6-k$.

N 能被 9 整除当且仅当 N 的各位数码之和能被 9 整除. 选到第 2004 位时，N 的前 2004 位数码之和为 $6\times\frac{2004}{2}=6012$ 是 9 的倍数. 无论 A 怎样选择第 2005 位数码，都不能使 N 的各位数码之和是 9 的倍数. 因此，B 获胜.

3. 对任意的正整数 n，有

$$11^n=(10+1)^n=\sum_{k=0}^{n}C_n^k10^k\equiv10n+1(\bmod 100).$$

故 11^n 的十位数字等于 n 的最后一位数字.

又因为 12^n 的末位数字为 2，4，8，6，2，4，… ($n=1$，2，…)，是以 4 为周期，所以，12^{13} 的末位数字为 2.

因此，$11^{12^{13}}$ 的十位数字为 2.

4. 首先注意到这样一个事实：对数 A 的各位数码无论如何重排，都不会使数 A 扩大 9 倍或更多倍，因此应有

$$\frac{2^n}{2^k}<9. \quad ①$$

此外，如果两个数具有相同的数码，则它们的差能被 9 整除，即有

$9|2^n-2^k$.

从而 $9|2^k(2^{n-k}-1)$，即 $9\mid2^{n-k}-1$.

但由①式可知　$2^{n-k}<9$，

因此 $2^{n-k}-1$ 不可能是 9 的倍数.

即不可能使 2^k 的各位数码重排得到 2^n $(n>k)$.

5. 假设 p^n 中的 20 个数码没有三个是相同的，则数码 0，1，2，…，9 在 p^n 中各出现 2 次.

计算 p^n 的各位数码之和为

$2(0+1+2+\cdots+9)=90$.

则 p^n 是 3 的倍数，从而 p 是 3 的倍数，又 p 是大于 3 的素数，这是不可能的.

所以在 p^n 的 20 位数码中必有三个是相同的.

6. 设 $s(m)$ 是正整数 m 的各位数字之和，题目要求回答的是：

是否存在一个正整数 n，使 $s(n\cdot s(n))=3$.

由于一个正整数能被 3 整除的充分必要条件是它的各位数字之和能被 3 整除. 因此，乘积 $n\cdot s(n)$ 一定能被 3 整除，所以，在 n 与 $s(n)$ 中，至少有一个能被 3 整除.

如果其中之一能被 3 整除，则另一个也能被 3 整除，于是，乘积 $n\cdot s(n)$ 一定能被 9 整除，从而，数 $s(n\cdot s(n))$ 也应该能被 9 整除. 因此，等式 $s(n\cdot s(n))=3$ 无解. 这表明，所求的正整数是

不存在的.

7. 3×3 的方格内各数字之和能被 4 整除只有两种情况：要么有 6 个 1，3 个 2，和为 12；要么有 2 个 1，7 个 2，和为 16.

因此，1 至少出现两次，2 至少出现 3 次.

在中间的 2×2 方格内任意填两个 1，其他填 2，其所有数字之和为 30，即为最大值；在中间的 2×2 方格内任意填三个 2，其他填 1，其所有数字之和为 19，即为最小值.

8. 因为要求$\overline{ab}$是 2 的倍数，$\overline{abcd}$是 4 的倍数，$\overline{abcdef}$是 6 的倍数，所以

b，d，$f\in\{2,4,6\}$，

a，c，$e\in\{1,3,5\}$.

又因为$\overline{abcde}$是 5 的倍数，所以 $e=5$.

这时第 1 位 a 与第 3 位 c 只能取 1 或 3，此时有 $a+c=4$.

因为$\overline{abc}$是 3 的倍数，则

$3\mid a+b+c=4+b$.

于是只能有 $b=2$.

这时，所求六位数只能从如下几个数中去寻找：

123456，123654，321456，321654.

经检验，由 $4\nmid 1234, 4\nmid 3214$，

所以只有 123654 与 321654 是满足题目要求的六位数.

9. $(\sqrt{2}+\sqrt{5})^{2000}=(7+2\sqrt{10})^{1000}$.

设 $a_n=(7+2\sqrt{10})^n+(7-2\sqrt{10})^n$，则

$a_0=2$，$a_1=14$.

注意到$\{a_n\}$是二阶递推数列，其特征方程为

$[t-(7+2\sqrt{10})][t-(7-2\sqrt{10})]=0$，即 $t^2-14t+9=0$.

故 $a_{n+2}-14a_{n+1}+9a_n=0$.

因此，$\{a_n\}$是整数数列.

计算数列前几项模 10 的余数：

$a_0\equiv2 \pmod{10}$，$a_1\equiv4 \pmod{10}$，$a_2\equiv8 \pmod{10}$，

$a_3\equiv6 \pmod{10}$，$a_4\equiv2 \pmod{10}$，$a_5\equiv4 \pmod{10}$.

注意到 $a_0\equiv a_4 \pmod{10}$，$a_1\equiv a_5 \pmod{10}$，由于$\{a_n\}$是二阶递推数列，则

$a_{n+4}\equiv a_n \pmod{10}$.

故 $a_{1000}\equiv a_{996}\equiv a_{992}\equiv\cdots\equiv a_0\equiv2 \pmod{10}$.

因为 $0<7-2\sqrt{10}<1$，则

$0<(7-2\sqrt{10})^{1000}<1$.

故$[(7+2\sqrt{10})^{1000}]=a_n-1\equiv1 \pmod{10}$.

所以，$(\sqrt{2}+\sqrt{5})^{2000}$的小数点前第一位数字是 1.

又 $0<7-2\sqrt{10}<0.9$，则

$0<(7-2\sqrt{10})^{1000}<0.1$.

故$\{(7+2\sqrt{10}^n\}=1-(7-2\sqrt{10})^n>0.9$.

所以，$(\sqrt{2}+\sqrt{5})^{2000}$的小数点后第一位数字是 9.

10. 设 5 位数 $N=\overline{a_1a_2a_3a_4a_5}$.

a_1 作百位的三位数有 $P_4^2=12$ 个，

a_1 作十位的三位数有 $P_4^2=12$ 个，

a_1 作个位的三位数有 $P_4^2=12$ 个.

于是依题意有

$$N=\overline{a_1a_2a_3a_4a_5}=(a_1+a_2+a_3+a_4+a_5)(100\cdot12+10\cdot12+12)$$
$$=1332(a_1+a_2+a_3+a_4+a_5).$$

由于 $9|1332$,则

$9|N=\overline{a_1a_2a_3a_4a_5}$.

从而 $9|(a_1+a_2+a_3+a_4+a_5)$.

于是 N 应是 $1332\cdot9=11988$ 的倍数.

因为 $15=1+2+3+4+5\leqslant a_1+a_2+a_3+a_4+a_5\leqslant9+8+7+6+5=35$，所以 $a_1+a_2+a_3+a_4+a_5$ 只能为 18 或 27.

(1) 当 $a_1+a_2+a_3+a_4+a_5=18$ 时，

$\overline{a_1a_2a_3a_4a_5}=1332\cdot18=23976$，

但是 $2+3+9+7+6=27\neq18$.

(2) 当 $a_1+a_2+a_3+a_4+a_5=27$ 时，

$\overline{a_1a_2a_3a_4a_5}=1332\cdot27=35964$，

此时 $3+5+9+6+4=27$.

所以，所求的五位数只有 35964.

11. 以 a 结尾的数形如 10^kb+a. 易知，a 稳定当且仅当 a^2 以 a 结尾，则有 $10^k|(a^2-a)$,即 $2^k5^k|a(a-1)$.

若 a 以 0 开始，我们定义 a 为相应正整数；若 a 的所有位上的数均为 0，记 a 为 0.

由于 a 与 $a-1$ 互素，有以下四种情形之一：

(1) $10^k|a$；

(2) $10^k|(a-1)$；

(3) $2^k|a,5^k|(a-1)$；

(4) $5^k|a,2^k|(a-1)$.

下面讨论这几种情形.

(1) 因为 $0\leqslant a<10^k$，所以，$a=\overline{0\cdots0}$.

(2) 因为 $-1\leqslant a-1<10^k$，所以，

$a-1=\overline{0\cdots0}$，即 $a=\overline{0\cdots01}$.

(3) 设 $a=2^kx$，$x\in\{1,2,\cdots,5^k-1\}$，$a-1=5^ky$，$y\in\mathbf{Z}$，则

$2^k x-5^k y=1.$ ①

显然，式①的所有解(x,y)满足

$$\begin{cases}x=x_0+5^k t, & ②\\ y=y_0+2^k t, & ③\end{cases}$$

其中(x_0,y_0)是式①的某个解，且$t\in\mathbf{Z}$.

因为$x_0\neq 0$，满足式②的等差级数在$[0,5^k)$内恰有一项，所以，式①恰有一组解(x_1,y_1)，其中，$x_1\in\{1,2,\cdots,5^k-1\}$. 由此，$a=2^k x_1\in\{1,2,\cdots,10^k-1\}$是所求的（若$a$的位数少于$k$，我们在$a$的左面加上相应个数的0）.

(4) 与 (3) 类似.

12. 首先证明对任意整数a，

$6\mid a^3-a.$

事实上，$a^3-a=(a-1)a(a+1)$是三个连续整数之积，因此它能被$3!=6$整除.

假设$a_1,a_2,\cdots,a_n$为n个整数，且

$6\mid a_1+a_2+\cdots+a_n.$

$(a_1^3+a_2^3+\cdots+a_n^3)-(a_1+a_2+\cdots+a_n)=(a_1^3-a_1)+(a_2^3-a_2)+\cdots+(a_n^3-a_n).$

由$6\mid a_i^3-a_i$，$i=1,2,\cdots,n$可得

$6\mid(a_1^3+a_2^3+\cdots+a_n^3)-(a_1+a_2+\cdots+a_n).$

因而$6\mid a_1^3+a_2^3+\cdots+a_n^3.$

13. 证法1 注意到

$$\begin{aligned}&n(n^2-1)(n^2-5n+26) \quad ①\\ =&(n+1)n(n-1)[(n^2+5n+6)-10n+20]\\ =&(n-1)n(n+1)(n+2)(n+3)-10(n+1)n(n-1)(n-2).\end{aligned}$$

因为$(n-1)n(n+1)(n+2)(n+3)$是5个连续正整数的积，其中至少有两个连续偶数，这两个偶数中必有一个是4的倍数，所以，这两个偶数的积是8的倍数.

因此，$(n-1)n(n+1)(n+2)(n+3)$是8的倍数.

又$(n-1)n(n+1)(n+2)(n+3)$是3和5的倍数，则$(n-1)n(n+1)(n+2)(n+3)$是$8\times3\times5=120$的倍数.

另外，$(n-2)(n-1)n(n+1)$又是3和4的倍数，从而是12的倍数.

所以，$10(n-2)(n-1)n(n+1)$是120的倍数.

综上，目标式①能被120整除.

证法2 注意到

$$\begin{aligned}n(n^2-1)(n^2-5n+26)&=n(n^2-1)[(n^2-5n+6)+20]\\ &=(n+1)n(n-1)(n-2)(n-3)+20(n-1)n(n+1).\end{aligned}$$

因为$(n+1)n(n-1)(n-2)(n-3)$是5个连续正整数的积，其中至少有两个连续偶数，这两个偶数中必有一个是4的倍数，所以，这两个偶数的积是8的倍数.

因此，$(n+1)n(n-1)(n-2)(n-3)$是8的倍数.

又$(n+1)n(n-1)(n-2)(n-3)$是3和5的倍数，则$(n+1)n(n-1)(n-2)(n-3)$是$8\times3\times5=$

120 的倍数.

另外，$(n-1)n(n+1)$又是 2 和 3 的倍数，从而是 6 的倍数.

所以，$20(n-1)n(n+1)$是 $20\times6=120$ 的倍数.

综上，目标式①能被 120 整除.

14. 由已知

$a_{n+2}=(n+3)a_{n+1}-(n+2)a_n$,

$a_{n+2}-a_{n+1}=(n+2)(a_{n+1}-a_n)$.

记 $b_{n+1}=a_{n+1}-a_n$,则有

$b_{n+1}=(n+1)b_n$.

由此易得 $b_n=n!$.

从而 $n!=a_n-a_{n-1}$,

$(n-1)!=a_{n-1}-a_{n-2}$,

……

$2!=a_2-a_1$.

诸式相加，再利用 $a_1=1$ 可得

$a_n=1!+2!+\cdots+n!$.

通过计算可得

$a_4=1+2!+3!+4!=33$,

所以 $11\mid a_4$.

$a_8=1+2!+3!+\cdots+8!=46233$,

所以 $11\mid a_8$.

又 $n\geqslant10$ 时，

$a_n=a_8+(9!+10!)+11!+12!+\cdots+n!=a_8+9!\cdot11+11!+12!+\cdots+n!$,

所以 $11\mid a_n(n\geqslant10)$.

于是，当 $n=4,n=8,n\geqslant10$ 时，$11\mid a_n$.

15. 证法 1 设表达式 $2x+3y$ 等于某个整数 k，即

$$2x+3y=k, \quad ①$$

这时有 $$x=\frac{k-3y}{2}=-y+\frac{k-y}{2}. \quad ②$$

因此，仅当$\frac{k-y}{2}$等于某个整数 s 时，x 才能是整数. 由$\frac{k-y}{2}=s$ 可得

$y=k-2s$.

再由②，

$x=-y+s=3s-k$.

因此，仅当

$$x=-k+3s,\ y=k-2s \quad ③$$

时，整数 x 和 y 才能满足等式①，这里 s 是任意整数.

反之，当 s 取任意整数时，由③可得整数 x 和 y，它们满足等式①.

又设

$$9x+5y=l, \quad ④$$

其中 l 为某个给定的整数.

这时同样可得

$$x=5t-l,\ y=-9t+2l, \quad ⑤$$

其中 t 是任意整数.

若表达式 $2x+3y$ 是 17 的倍数，由①和③有

$$x=-17n+3s,\ y=17n-2s,$$

其中 s 为任意整数.

这时有

$$9x+5y=9(-17n+3s)+5(17n-2s)=17(-4n+s),$$

于是 $9x+5y$ 也是 17 的倍数.

同样，若 $9x+5y$ 是 17 的倍数，由④和⑤有

$$x=5t-17m,\ y=-9t+34m,$$

从而可得

$$2x+3y=2(5t-17m)+3(-9t+34m)=17(-t+4m),$$

于是 $2x+3y$ 也是 17 的倍数.

证法 2　设 $u=2x+3y$，$v=9x+5y$.

当 x 和 y 是整数时，u 和 v 也是整数.

于是　$3v-5u=17x$.　①

当 $2x+3y$ 能被 17 整除时，即 u 能被 17 整除时，由①式，$3v$ 能被 17 整除，又由 3 和 17 互素，则 v 能被 17 整除，即 $9x+5y$ 能被 17 整除.

当 $9x+5y$ 能被 17 整除时，即 v 能被 17 整除，由①式，$5u$ 能被 17 整除，又由 5 和 17 互素，则 u 能被 17 整除，即 $2x+3y$ 能被 17 整除.

16. 解法 1　如果一个正整数的立方以 8 结尾，那么这个数本身必以 2 结尾，即它可以写成

$n=10k+2$（k 为非负整数）

的形式，于是

$$n^3=(10k+2)^3=1000k^3+600k^2+120k+8.$$

其中 $120k$ 决定了 n^3 的十位数码.

由于要求 n^3 的十位数码是 8，则 $12k$ 的个位数应是 8，即 k 的个位是 4 或 9，因此可设

$k=5m+4$（m 为非负整数）.

这时 $n^3=[10(5m+4)+2]^3=125000m^3+315000m^2+264600m+74088.$

为使 n^3 的百位数字是 8，必须使 $2646m$ 的个位是 8，最小的 $m=3$.

这时　$k=5m+4=19$，$n=10k+2=192$.

可以求出 $n^3=7077888$，其末三位是 888.

因此所求的最小的 n 为 192.

解法 2　由题意有 $1000|n^3-888$，所以

$1000|n^3+112-1000$，从而

$1000|n^3+112$.

所以 n 是偶数，设 $n=2k$，则

$1000|8k^3+112=8(k^3+14)$.

这就需要 $125|k^3+14$.

首先必须 $5|k^3+14$，因此 k 的个位数字是 6 或 1.

于是可设 $k=5m+1$（m 为非负整数）.

$k^3+14=(5m+1)^3+14=125m^3+75m^2+15m+15=5(25m^3+15m^2+3m+3)$.

为使 $125|k^3+14$，只须

$25|15m^2+3m+3$，

从而 $15m^2+3m+3$ 的个位是 0 或 5. 由于

$15m^2+3m+3=3m(5m+1)+3$，

$m(5m+1)$一定为偶数，所以 $3m(5m+1)$的个位数一定为 2. 从而 $m(5m+1)$的个位一定是 4，此时 m 的个位一定是 4 或 9. 为此设 $m=5t+4$，（t 为非负整数）.

$$
\begin{aligned}
15m^2+3m+3&=15(5t+4)^2+3(5t+4)+3=15\cdot 25t^2+40\cdot 15t+16\cdot 15+15t+15\\
&=15\cdot 25t^2+24\cdot 25t+15t+15\cdot 17.
\end{aligned}
$$

为使 $25|15m^2+3m+3$，只须

$25|15t+15\cdot 17$，即 $5|3t+51$.

取最小的 $t=3$.

于是　$m=5t+4=19$，$k=5m+1=96$.

从而　$n=2k=192$.

17. 由于 $34!=K\cdot 11^3\cdot 7^4\cdot 5^7\cdot 3^{15}\cdot 2^{32}=K\cdot 11^3\cdot 7^4\cdot 3^{15}\cdot 2^{25}\cdot 10^7$，所以 $b=0$，$a\neq 0$.

考虑去掉最后面的 7 个零时的情形，知该数可以被 2^{25} 整除，也可以被 8 整除，即最后三位数 $\overline{35a}$ 可以被 8 整除（因为 1000 可以被 8 整除），因此 $a=2$.

由于 34! 可以被 9 整除，所以各位数字之和也可以被 9 整除，于是 $141+c+d\equiv 0 \pmod 9$，即 $c+d\equiv 3 \pmod 9$.

而 34! 还可以被 11 整除，所以，奇数位与偶数位上数字之和的差可以被 11 整除. 于是

$80+d\equiv 61+c \pmod{11}$，即 $8+d\equiv c \pmod{11}$.

当 $c+d=3$，$8+d=c$ 时，无解；

当 $c+d=12$，$8+d=c$ 时，无解；

当 $c+d=12$，$d=3+c$ 时，无解；

当 $c+d=3$，$d=c+3$ 时，得 $c=0$，$d=3$.

综上所述，$a=2$，$b=0$，$c=0$，$d=3$.

第八章　平方数

1. 设 $\sqrt{k^2-pk}=n$，$n\in \mathbf{N}^*$，则 $k^2-pk-n^2=0$，$k=\dfrac{p\pm\sqrt{p^2+4n^2}}{2}$，从而 p^2+4n^2 是平方数，

设为 m^2，$m\in\mathbf{N}^*$，则 $(m-2n)(m+2n)=p^2$.

因为 p 是素数，且 $p\geqslant3$，所以 $\begin{cases}m-2n=1,\\m+2n=p^2,\end{cases}$ 解得 $\begin{cases}m=\dfrac{p^2+1}{2},\\n=\dfrac{p^2-1}{4}.\end{cases}$

所以 $k=\dfrac{p\pm m}{2}=\dfrac{2p\pm(p^2+1)}{4}$，故 $k=\dfrac{(p+1)^2}{4}$(负值舍去).

2. 设 $n^2+59n+881=m^2$ (m 为整数)，则

$4m^2=(2n+59)^2+43$，即 $(2m+2n+59)(2m-2n-59)=43$.

因为 43 为素数，所以，

$\begin{cases}2m+2n+59=43,-43,1,-1,\\2m-2n-59=1,-1,43,-43.\end{cases}$

解得 $n=-40$ 或 -19.

3. 设 $n^2+2007n=m^2$ ($m\in\mathbf{N}_+$).

故存在正整数 k，满足 $m=n+k$，因此，

$n^2+2007n=(n+k)^2$，即 $n=\dfrac{k^2}{2007-2k}$.

故 $2007-2k>0$，$k\leqslant1003$，且

$(2007-2k)\mid k^2$.

为使 n 取最大值，分子 k^2 应尽可能大，而分母尽可能小.

故当 $k=1003$ 时，$n=\dfrac{1003^2}{1}=1006009$ 为其最大值.

4. 注意到

$2^4+2^7=144=12^2$.

令 $144+2^n=m^2$，其中 m 为正整数，则

$2^n=m^2-144=(m-12)(m+12)$.

上式右边的每个因式必须为 2 的幂，设

$m+12=2^p$, ①

$m-12=2^q$, ②

其中 p，$q\in\mathbf{N}$，$p+q=n$，$p>q$.

①−②得

$2^q(2^{p-q}-1)=2^3\times3$.

因为 $2^{p-q}-1$ 为奇数，2^q 为 2 的幂，所以，等式仅有一个解，即 $q=3$，$p-q=2$.

因此，$p=5$，$q=3$.

故 $n=p+q=8$ 是使所给表达式为完全平方数的唯一正整数.

5. 因为 $5=1^2+2^2$，$401=1^2+20^2$，所以，

$2005=5\times401=|2+i|^2|20+i|^2=|(2+i)(20+i)|^2=|39+22i|^2=39^2+22^2$.

故 $2005^{2005}=(39\times2005^{1002})^2+(22\times2005^{1002})^2$ 是两个完全平方数的和.

因为完全立方数模 7 的余数只能是 0，±1，所以，两个完全立方数的和模 7 的余数只能是 0，±1，±2.

但 $2005^{2005}\equiv3^{2005}=(3^6)^{334}\times3\equiv3 \pmod 7$，

所以，2005^{2005} 不是两个完全立方数的和.

6. 设 $100a+b=m^2$，$201a+b=n^2$，则

$101a=n^2-m^2=(n-m)(n+m)$，$m,n<100$.

所以，$n-m<100$，$n+m<200$，$101\mid(m+n)$.

从而，$m+n=101$.

代入 $a=n-m=2n-101$，得

$201(2n-101)+b=n^2$，即 $n^2-402n+20301=b\in(9,100)$.

经验证 $n=59$，$m=101-n=42$.

从而，$a=n-m=17$，$b=n^2-402n+20301=64$，即 $(a,b)=(17,64)$.

7. 只要证明：对于每个满足 $p\mid ab$ 的素数 p，存在正整数 m，使得 $p^{3m}\parallel ab$.

设 $p^k\parallel a$，$p^l\parallel b$，$p^{k+l}\parallel ab$.

(1) 若 $k=l$，则 $p^{2k}\parallel(a^3+b^3+ab)$，而 $p^{3k}\mid ab(a-b)$，矛盾.

(2) 若 $k>l$，则 $p^{k+2l}\parallel ab(a-b)$，$p^{3k}\parallel a^3$，$p^{3l}\parallel b^3$，$p^{k+l}\parallel ab$. 而 $3l,k+l<k+2l$，由 $ab(a-b)\mid(a^3+b^3+ab)$，得

$p^{k+2l}\mid(a^3+b^3+ab)$，

$p^{k+2l}\mid(b^3+ab)=p^{3l}b_1^3+p^{k+l}a_1b_1$.

因此，一定有 $3l=k+l$，即 $k=2l$.

故 $p^{3l}\parallel ab$，其中，$b=p^lb_1$，$p\nmid b_1$；$a=p^ka_1$，$p\nmid a_1$.

同理，可证 $k<l$ 的情形.

8. **解法 1** 只需证 $p^2-1=(p-1)(p+1)$ 能被 24 整除.

因为 p 为大于 3 的素数，且 p 为奇数，所以，$p-1$ 与 $p+1$ 为两个连续的偶数，且其中之一为 4 的倍数. 故 $(p-1)(p+1)$ 能被 8 整除.

又因为在 3 个连续的整数 $p-1$，p，$p+1$ 中必有一个是 3 的倍数，且 p 为大于 3 的素数，所以，$(p-1)(p+1)$ 为 3 的倍数.

而 $(8,3)=1$，故 $p^2-1=(p-1)(p+1)$ 能被 24 整除.

解法 2 因大于 3 的素数均可以表示成 $6k\pm1$ 的形式，所以，

$p^2-1=(6k\pm1)^2-1=12k(3k\pm1)$.

又因为 k 与 $3k\pm1$ 的奇偶性不同，则它们的积为偶数，所以，p^2-1 能被 24 整除.

9. 显然，n 是非负整数. 当 k，l，m 都是 2 的倍数时，等式两边同时除以 2 的幂，使得 k，l，m 不全是偶数. 因此，可以假设 k，l，m 不全是偶数.

因完全平方数模 4 余 0 或 1，故 $k^2+l^2+m^2$ 模 4 余 1，2，3.

所以，2^n 不能被 4 整除，n 只能取 0 或 1.

当 $n=0$ 时，$k^2+l^2+m^2=1$，此时解为 $(k,l,m)=(0,0,1)$ 或这些数的置换.

当 $n=1$ 时，$k^2+l^2+m^2=2$，此时解为 $(k,l,m)=(0,1,1)$ 或这些数的置换.

因此，原题的解是$(0,\pm2^k,\pm2^k)$，或$(0,0,\pm2^k)$或这些数的置换，前者$n=2k+1$，后者$n=2k$，$k\in\mathbf{N}$.

10. 因为$A=\frac{4}{9}\times\underbrace{99\cdots9}_{2n个}=\frac{4}{9}\times(10^{2n}-1)$，

$B=\frac{8}{9}\times\underbrace{99\cdots9}_{n个}=\frac{8}{9}\times(10^n-1)$，

$$故\ A+2B+4=\frac{4}{9}\times(10^{2n}-1)+\frac{16}{9}\times(10^n-1)+4=\frac{4}{9}\times10^{2n}+\frac{16}{9}\times10^n+\frac{16}{9}$$

$$=\left(\frac{2}{3}\times10^n+\frac{4}{3}\right)^2.$$

又因为$2\times10^n+4\equiv2\times1+1\equiv0(\mathrm{mod}\ 3)$，因此，$\frac{2}{3}\times10^n+\frac{4}{3}$是整数.

所以，$A+2B+4$是一个完全平方数.

11. 倒数第17位数为7的数居多.

将每个不超过10^{20}的完全平方数都写成一个20位数（若不足20位，则在前面空缺的位置上补0），再把它们分为1000组，使得每一组内的数的最前面三位数字彼此相同. 只须证明，在每一组内，第四位数为7的数都比第四位数为8的数多.

为此，将左闭右开区间$[(A-1)\cdot10^{16},A\cdot10^{16})$中的完全平方数的个数与左闭右开区间$[A\cdot10^{16},(A+1)\cdot10^{16})$中的完全平方数的个数相比较，其中$A<10^4$是任何一个个位数为8，前面三位数字任取的正整数.

显然，它们分别等于区间

$[\sqrt{A-1}\cdot10^8,\sqrt{A}\cdot10^8)$和$[\sqrt{A}\cdot10^8,\sqrt{A+1}\cdot10^8)$

中的正整数的个数. 众所周知，区间$[a,b)$中的正整数的个数与区间的长度$b-a$的差不超过1. 故只须证明，所考察的两个区间的长度之差大于2. 而这是因为

$$(\sqrt{A}\cdot10^8-\sqrt{A-1}\cdot10^8)-(\sqrt{A+1}\cdot10^8-\sqrt{A}\cdot10^8)$$

$$=10^8[(\sqrt{A}-\sqrt{A-1})-(\sqrt{A+1}-\sqrt{A})]$$

$$=10^8\left(\frac{1}{\sqrt{A}+\sqrt{A-1}}-\frac{1}{\sqrt{A+1}+\sqrt{A}}\right)$$

$$=10^8\left[\frac{\sqrt{A+1}-\sqrt{A-1}}{(\sqrt{A}+\sqrt{A-1})(\sqrt{A+1}+\sqrt{A})}\right]$$

$$=\frac{2\times10^8}{(\sqrt{A+1}+\sqrt{A-1})(\sqrt{A}+\sqrt{A-1})(\sqrt{A+1}+\sqrt{A})}$$

$$>\frac{2\times10^8}{2\sqrt{10^4}\times2\sqrt{10^4}\times2\sqrt{10^4}}=25>2.$$

12. $n=1,2,3,6,7,15$.

首先，证明对于所有的$n\geqslant17$，有多于2个不同的表达式.

因为每个正整数都可以表示为4个或不足4个的正整数的平方和（拉格朗日四平方定理），于是，存在非负整数x_i，y_i，z_i，w_i（$i=1,2,3,4$）满足

$n-0^2=x_0^2+y_0^2+z_0^2+w_0^2$,

$n-1^2=x_1^2+y_1^2+z_1^2+w_1^2$,

$n-2^2=x_2^2+y_2^2+z_2^2+w_2^2$,

$n-3^2=x_3^2+y_3^2+z_3^2+w_3^2$,

$n-4^2=x_4^2+y_4^2+z_4^2+w_4^2$.

由此得

$$n=x_0^2+y_0^2+z_0^2+w_0^2=1^2+x_1^2+y_1^2+z_1^2+w_1^2=2^2+x_2^2+y_2^2+z_2^2+w_2^2$$
$$=3^2+x_3^2+y_3^2+z_3^2+w_3^2=4^2+x_4^2+y_4^2+z_4^2+w_4^2.$$

假设 $n\neq1^2+2^2+3^2+4^2=30$，则有

$\{1,2,3,4\}\neq\{x_0,y_0,z_0,w_0\}$.

所以，存在 $k\in\{1,2,3,4\}\setminus\{x_0,y_0,z_0,w_0\}$，且对这样的 k，

$x_0^2+y_0^2+z_0^2+w_0^2$ 和 $k^2+x_k^2+y_k^2+z_k^2+w_k^2$ 是 n 的不同的表达式.

因为 $30=1^2+2^2+3^2+4^2=1^2+2^2+5^2$，只要考虑 $1\leqslant n\leqslant16$ 即可.

下面这些正整数有两种（或更多）不同的表达式：

$4=2^2=1^2+1^2+1^2+1^2$,

$5=1^2+2^2=1^2+1^2+1^2+1^2+1^2$,

$8=2^2+2^2=1^2+1^2+1^2+1^2+2^2$,

$9=3^2=1^2+2^2+2^2$,

$10=1^2+3^2=1^2+1^2+2^2+2^2$,

$11=1^2+1^2+3^2=1^2+1^2+1^2+2^2+2^2$,

$12=1^2+1^2+1^2+3^2=2^2+2^2+2^2$,

$13=1^2+1^2+1^2+1^2+3^2=1^2+2^2+2^2+2^2$,

$14=1^2+2^2+3^2=1^2+1^2+2^2+2^2+2^2$,

$16=4^2=2^2+2^2+2^2+2^2$.

而 1，2，3，6，7，15 这六个正整数仅有唯一的表达式：

$1=1^2$，$2=1^2+1^2$，$3=1^2+1^2+1^2$，$6=1^2+1^2+2^2$，

$7=1^2+1^2+1^2+2^2$，$15=1^2+1^2+2^2+3^2$.

因此，所求的正整数 n 为 1，2，3，6，7，15.

13. 因 $44x\geqslant86868$，故

$$x\geqslant\left[\frac{86868+43}{44}\right]=1975.$$

从而 x 至少为四位数.

另一方面，若 x 的位数 $k\geqslant5$，则

$44x-86868>4\times10^k-10^5\geqslant3\times10^k>9^k$，

于是得 $44x-86868>p(x)$（x 的 k 个数字之积），矛盾，故 x 恰为四位数.

由已知 x 的四位数字之和 $S(x)$ 满足 $1\leqslant S(x)\leqslant36$，故 $S(x)=1,8$ 或 27.

显然 $S(x)=1$ 不合要求.

因为 $0<p(x)\leqslant 9^4=6561$，所以

$$x\leqslant\left[\frac{86868+6561}{44}\right]=2123.$$

而满足 $1975\leqslant x\leqslant 2123$ 且使 $S(x)=8$ 或 27，$p(x)\neq 0$ 的 x 只有 1989，1998，2114，2123 四个，经检验只有 $x=1989$ 的各位数字的积等于 $44x-86868$，因此 $x=1989$ 是本题的唯一解.

14. 因为 $9(2a+b)^2-3^2(2a+b)^2$ 为完全平方数，所以，$509(4a+511b)$ 为完全平方数. 而 509 为素数，可令

$$4a+511b=509\times 3^2k^2. \quad ①$$

于是，原等式变为

$9(2a+b)^2=509^2\times 3^2k^2$，即 $2a+b=509k$.

从而，$b=509k-2a$，代入式①得

$4a+511(509k-2a)=509\times 3^2k^2$，

解得 $a=\dfrac{k(511-9k)}{2}$.

因为 a 为素数，即 $\dfrac{k(511-9k)}{2}$ 为素数，所以，有以下几种情况：

(1) 当 $k=1$ 时，$a=\dfrac{k(511-9k)}{2}=\dfrac{511-9}{2}=251$ 为素数，符合条件，此时，

$b=509k-2a=509-502=7$.

(2) 当 $k=2$ 时，$a=\dfrac{k(511-9k)}{2}=511-18=493=17\times 29$ 不为素数，舍去.

(3) 当 $k>2$，且 k 为奇数时，因为 $a=\dfrac{k(511-9k)}{2}=k\cdot\dfrac{511-9k}{2}$ 为素数，而 $k>1$，所以，$\dfrac{511-9k}{2}=1$. 但 $\dfrac{511-9k}{2}=1$ 无整数解，舍去.

(4) 当 $k>2$，且 k 为偶数时，因为 $a=\dfrac{k(511-9k)}{2}=\dfrac{k}{2}(511-9k)$ 为素数，而 $\dfrac{k}{2}>1$，所以，$511-9k=1$. 但 $511-9k=1$ 无整数解，舍去.

综上所述，$a=251$，$b=7$.

15. 采用反证法，设 $n^7+7=x^2$ 对某个正整数对 (n,x) 成立，则

(1) n 为奇数，否则导致 $x^2\equiv 3\pmod 4$，矛盾！

(2) $n\equiv 1\pmod 4$，这是因为 n 为奇数，故 $4\mid n^7+7$，因此 $n\equiv 1\pmod 4$.

(3) 由 $x^2=n^7+7$ 可得

$$x^2+11^2=n^7+128=(n+2)(n^6-2n^5+4n^4-8n^3+16n^2-32n+64). \quad ①$$

现在，若 $11\nmid x$，则 x^2+11^2 的每一个素因子 p 都为奇数，且 $p\equiv 1\pmod 4$. 这是因为若 $p\equiv 3\pmod 4$，设 $p=4k+3$，则由 $x^2\equiv -11^2\pmod p$ 两边 $2k+1$ 次方，得

$$x^{p-1}\equiv -11^{p-1}\equiv -1\pmod p,$$

矛盾！(这里用到 Fermat 小定理)

但由①知 $n+2\mid x^2+11^2$，而 $n+2\equiv 3\pmod 4$，它至少有一个模 4 余 3 的素因子，这与 x^2+

11^2 的每一个素因子 p 都满足 $p\equiv1\pmod 4$ 矛盾.

若 x 为 11 的倍数，设 $x=11y$，则①变为

$121(y^2+1)=(n+2)(n^6-2n^5+4n^4-8n^3+16n^2-32n+64)$，

依次将 $n\equiv0$，±1，±2，…，$\pm5\pmod{11}$ 分别代入直接计算，可知 $n^6-2n^5+4n^4-8n^3+16n^2-32n+64$ 不是 11 的倍数，所以 $121\mid(n+2)$，这表明

$$y^2+1=\frac{n+2}{121}(n^6-2n^5+4n^4-8n^3+16n^2-32n+64). \qquad ②$$

与前类似可证：y^2+1 的每个素因子都模 4 余 1，因此其每个奇约数都模 4 余 1，但 $\frac{n+2}{121}\equiv3\pmod 4$，所以②不能成立.

综上，n^7+7 不是一个完全平方数.

16．设 p 为奇素数，则 $\left(\frac{p+1}{2}\right)^2$ 是好平方数$\left[因为\left(\frac{p+1}{2}\right)^2=p+\left(\frac{p-1}{2}\right)^2\right]$.

又奇素数 p 有无数个，从而，好平方数有无数个.

设 n 为正整数.

下面证明：$(3n+2)^2$ 是坏平方数.

实际上，反设存在正整数 x 及素数 p，使 $(3n+2)^2=x^2+p$，则

$p=(3n+2)^2-x^2=(3n+2+x)(3n+2-x)$.

而 p 是素数，因此，

$3n+2-x=1$，$3n+2+x=p$.

解得 $p=3(2n+1)$，与 p 是素数矛盾.

因为正整数 n 有无数个，所以，坏平方数有无数个.

17．证法 1　不失一般性，不妨设 S 中只含有正整数.

设 $S=\{2^{a_i}3^{b_i}\mid a_i,b_i\in\mathbf{Z},a_i,b_i\geqslant0,1\leqslant i\leqslant9\}$.

只需证明存在 $1\leqslant i_1,i_2,i_3\leqslant9$，使得

$a_{i_1}+a_{i_2}+a_{i_3}\equiv b_{i_1}+b_{i_2}+b_{i_3}\equiv0\pmod 3$.

对 $n=2^a3^b\in S$，称 $(a\pmod 3,b\pmod 3)$ 为 n 的类型，则共有以下 9 种类型：

$(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)$.

记 S 中类型 (i,j) 的元素个数为 $N(i,j)$.

当 $N(i,j)$ 满足以下四个条件之一时，可得到乘积为完全立方数的 3 个不同的整数：

(1) 存在 (i,j)，使得 $N(i,j)\geqslant3$；

(2) 存在 $i\in\{1,2,3\}$，使得 $N(i,0)N(i,1)N(i,2)\neq0$；

(3) 存在 $j\in\{1,2,3\}$，使得 $N(0,j)N(1,j)N(2,j)\neq0$；

(4) $N(i_1,j_1)N(i_2,j_2)N(i_3,j_3)\neq0$，其中，$\{i_1,i_2,i_3\}=\{j_1,j_2,j_3\}=\{0,1,2\}$.

假设条件 (1)，(2)，(3) 均不满足.

由于对所有的 (i,j)，均有 $N(i,j)\leqslant2$，因此，存在至少 5 个非零的 $N(i,j)$. 此外，对这些非零的 $N(i,j)$，不存在某三个的 i 值或 j 值相同.

根据这些条件，易知条件 (4) 必然满足［例如，在 3×3 的方阵中，行和列均按 0，1，2 标

记，将所有的非零的 $N(i,j)$ 填入第 i 行第 j 列，那么，总可以在该方阵中找到三个元素，它们的行和列都不同，此即（4）].

证法 2 对 $n=2^a3^b\in S$，同证法 1 得到 9 种 n 的类型.

注意到以下两点：

(1) 对任意 5 个整数，总存在 3 个数之和能被 3 整除；

(2) 对 i，j，$k\in\{0,1,2\}$，$i+j+k\equiv0\pmod 3$ 当且仅当 $i=j=k$ 或 $\{i,j,k\}=\{0,1,2\}$.

用 T 表示 S 中整数的类型的集合，$N(i)$ 表示 S 中类型为 $(i,\cdot)$ 的整数的个数，$M(i)$ 表示使得 $(i,j)\in T$ 的整数 $j\in\{0,1,2\}$ 的个数.

若对某些 i，有 $N(i)\geqslant5$，则由（1）知结论成立. 否则，对于 $\{0, 1, 2\}$ 的某些排列不成立.

18. 设正整数 a 满足 $d=d(a)=a^2$，且 a 有 $n+1$ 位数字，$n\geqslant0$. 又设 a 的最后一位数字为 s，c 的第一位数字为 f. 因为

$(*\cdots*s)^2=a^2=d=*\cdots*f$，

$(s*\cdots*)^2=b^2=c=f*\cdots*$，

其中 $*$ 表示一位数字，所以，f 既是末位数字为 s 的一个数的平方的最后一位数字，又是首位数字为 s 的一个数的平方的第一位数字.

完全平方数 $a^2=d$ 要么是 $2n+1$ 位数，要么是 $2n+2$ 位数.

若 $s=0$，则 $n\neq0$，b 有 n 位数字，其平方 c 最多有 $2n$ 位数字. 所以，d 也最多有 $2n$ 位数字，矛盾.

因此，a 的最后一位数字不是 0.

若 $s=4$，则 $f=6$. 因为首位数字为 4 的数的平方的首位数字为 1 或 2，即

$160\cdots0=(40\cdots0)^2\leqslant(4*\cdots*)^2<(50\cdots0)^2=250\cdots0$，

所以，$s\neq4$.

下表给出了 s 所有可能的情况下对应的 f 的取值情况：

s	1	2	3	4	5	6	7	8	9
$f=(\cdots s)^2$ 的末位数字	1	4	9	6	5	6	9	4	1
$f=(\cdots s)^2$ 的首位数字	1,2,3	4,5,6,7,8	9,1	1,2	2,3	3,4	4,5,6	6,7,8	8,9

从上表可看出，$s=1$，$s=2$，$s=3$ 时，均有 $f=s^2$.

当 $s=1$ 或 $s=2$ 时，$n+1$ 位且首位数字为 s 的数 b 的平方 $c=b^2$ 是 $2n+1$ 位数；当 $s=3$ 时，$c=b^2$ 要么是首位数字是 9 的 $2n+1$ 位数，要么是首位数字是 1 的 $2n+2$ 位数. 由 $f=s^2=9$ 知首位数字不可能是 1，所以，c 一定是 $2n+1$ 位数.

设 $a=10x+s$，其中 x 是 n 位数（特别地，$x=0$，设 $n=0$），则

$b=10^ns+x$，$c=10^{2n}s^2+2\times10^nsx+x^2$，

$d-10(c-10^{m-1}f)+f=10^{2n+1}s^2+20\times10^n sx+10x^2-10^n f+f$,

其中 m 是数 c 的位数，且已知 $m=2n+1$，$f=s^2$.

故 $d=20\times10^n sx+10x^2+s^2$.

由 $a^2=d$，解得 $x=2s\cdot\frac{10^n-1}{9}$.

于是，$a=6\underbrace{\cdots}_{n个}63$，$a=4\underbrace{\cdots}_{n个}42$ 或 $a=2\underbrace{\cdots}_{n个}21$，其中 $n\geqslant0$.

对于前两种可能的情况，若 $n\geqslant1$，由 a^2-d，得 d 有 $2n+2$ 位数字，这表明 c 也有 $2n+2$ 位数字．这与 c 有 $2n+1$ 位数字矛盾，因此，$n=0$.

综上所述，满足条件的数 a 分别为

$a=3$，$a=2$，$a=2\underbrace{\cdots}_{n个}21$，其中 $n\geqslant0$.

第九章　公约数和公倍数

1. 设 100 个正整数 a_1，a_2，…，a_{100}的最大公约数为 d，并令

$a_j=da_j'(1\leqslant j\leqslant100)$.

由于 $a_1+a_2+\cdots+a_{100}=d(a_1'+a_2'+\cdots+a_{100}')=101101=101\cdot1001$，于是

a_1'，a_2'，…，a_{100}'不可能都是 1，从而

$a_1'+a_2'+\cdots+a_{100}'\geqslant1\cdot99+2=101$.

从而　$d\leqslant1001$.

另一方面，取 $a_1=a_2=\cdots=a_{99}=1001$，$a_{100}=2002$，这时满足

$a_1+a_2+\cdots+a_{100}=101101$.

而$(1001,1001,\cdots,1001,2002)=1001$，

所以 a_1，a_2，…，a_{100}的最大公约数的最大可能值为 1001.

2. 设所求的数为 x 和 y，且 $d=(x,y)$，则

$x=dx_1,y=dy_1,(x_1,y_1)=1$.

于是　$[x,y]=\frac{xy}{d}=dx_1y_1$.

由题意，有

$$\begin{cases}d(x_1+y_1)=667, & ①\\ \frac{dx_1y_1}{d}=120. & ②\end{cases}$$

由　$x_1y_1=120=2^3\cdot3\cdot5$，

又　$667=1\cdot23\cdot29$，

因此由①，②可得

$x_1=8$，$y_1=15$，或 $x_2=24$，$y_2=5$.

相应的 $d_1=29$，$d_2=23$.

因此，所求的数有两组：

$x_1=232$，$y_1=435$，或 $x_2=552$，$y_2=115$.

3. 由于55是5与11的最小公倍数，所以，在不大于55的正整数中，恰有 $11+5-1=15$ 个数能被5或11整除. 这些数是：

$a_1=5$，$a_2=10$，$a_3=11$，$a_4=15$，$a_5=20$，$a_6=22$，$a_7=25$，$a_8=30$，

$a_9=33$，$a_{10}=35$，$a_{11}=40$，$a_{12}=44$，$a_{13}=45$，$a_{14}=50$，$a_{15}=55$.

又由于 $2004=133\times15+9$，于是，所要找的数为

$133\times55+a_9=133\times55+33=7348$.

4. 令 $N=9a^2+9b^2+9c^2$.

如果 a，b，c 都是3的倍数，则 N 可被81整除，与题意相矛盾.

于是，可设 a 不是3的倍数.

如果 $a+b+c$ 是3的倍数，则将 a 换为 $-a$，原表达式不变，所以，可设 $a+b+c$ 不是3的倍数.

注意到

$N=9a^2+9b^2+9c^2=(2a+2b-c)^2+(2b+2c-a)^2+(2c+2a-b)^2$，

其中，$2a+2b-c=2(a+b+c)-3c$ 不是3的倍数.

同理，其余两个整数也都不是3的倍数.

5. 由已知 $1059\equiv1417\equiv2312 \pmod d$，则

$d\mid2312-1417=895$，

$d\mid1417-1059=358$.

而 $(895,358)=179$，所以有 $d\mid179$.

又因为179是素数，$d>1$，所以

$d=179$.

再由 $1059=179\cdot5+164$，于是 $r=164$.

$d-r=179-164=15$.

6. 设 $[d_1,d_2]$ 表示 d_1，d_2 的最小公倍数，P_j 是所有题设的公差为 d_j $(j=1, 2)$ 的等差数列的并，$S=P_1\cap P_2$，于是，S 是具有公差 $[d_1,d_2]$ 的一个等差数列.

设 y 是 P_1 的最小元素，x 是 S 的最小元素.

注意到公差为 d_1 的任2个等差数列至少有2个公共元素，故 $b\leqslant k-1$.

将 a，b 的最大公因数记作 $\gcd(a,b)$.

若 $\dfrac{d_2}{\gcd(d_1,d_2)}\leqslant\dfrac{k}{2}$，则从 $b\leqslant k-1$ 可得出结果.

若 $\dfrac{d_2}{\gcd(d_1,d_2)}>\dfrac{k}{2}$，令

$m_0=2\dfrac{d_2}{\gcd(d_1,d_2)}-k$.

公差为 d_1 的每一个等差数列至少包含 S 的2个元素，且从 $x+md_1$ $(0\leqslant m\leqslant k-2)$ 开始. 而公差为 d_1、第一项为 $x+d_1$，$x+2d_1$，…，$x+m_0d_1$ 之一的等差数列只包含 S 的1个元素，即 $x+[d_1,d_2]$.

因此，$b\leqslant k-1-m_0=2\left[k-\dfrac{d_2}{\gcd(d_1,d_2)}\right]-1$.

7. (1) 设任意一对不考虑次序的正整数对$(m,n)(m、n\in\{1,2,\cdots,k\})$对应的素数为$\varphi(m,n)$，其中$m\neq n$，且若数对$(m,n)$和$(m_1,n_1)$不同，则

$\varphi(m,n)\neq\varphi(m_1,n_1)$.

设$a_i=\prod\limits_{\substack{n=1\\n\neq i}}^{k}\varphi(i,n),i=1,2,\cdots,k$,则

集合$\{a_1,a_2,\cdots,a_k\}$满足要求的条件.

因为a_i和a_j的最大公因数为$\varphi(i,j)$，a_i,a_l的最大公因数为$\varphi(i,l)$，其中$\varphi(i,j)$，$\varphi(i,l)$为不同的素数，因此，a_i，a_j，a_l的最大公因数为1，故对于所有的k $(k\geqslant3)$，均满足条件.

(2) 不存在满足条件的集合. 假设存在满足条件的集合$\{a_1,a_2,\cdots\}$，则显然有$a_1>1$.

设$a_1=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$，其中$p_1$，$p_2$，…，$p_s$是不同的素数. 考虑其中的$s+1$个数$a_2$，$a_3$，…，$a_{s+2}$. 因为这$s+1$个数中的每一个均与$a_1$不互素，因此，每一项均能被$p_1$，$p_2$，…，$p_s$之一整除. 所以，存在两个数，不妨设为$a_m$和$a_n$，这两个数均能被$p_i$整除. 于是，$a_1$，$a_m$，$a_n$不互素. 矛盾.

8. 当$m=n=1$时，由已知条件可得$f^2(1)+f(1)$是$(1^2+1)^2=4$的正因数. 因为$t^2+t=4$无整数根，且$f^2(1)+f(1)$比1大，所以，

$f^2(1)+f(1)=2$.

从而，$f(1)=1$.

当$m=1$时，有

$$(f(n)+1)\mid(n+1)^2, \quad ①$$

其中n为任意正整数.

同理，当$n=1$时，有

$$(f^2(m)+1)\mid(m^2+1)^2, \quad ②$$

其中m为任意正整数.

要证明$f(n)=n$，只须证明有无穷多个正整数k，使得$f(k)=k$. 实际上，若这个结论是对的，对于任意一个确定的$n\in\mathbf{N}_+$和每一个满足$f(k)=k$的正整数k，由已知条件可得

$k^2+f(n)=f^2(k)+f(n)$

整除$(k^2+n)^2$.

又$(k^2+n)^2=[(k^2+f(n))+(n-f(n))]^2=A(k^2+f(n))+(n-f(n))^2$，

其中A为整数.

于是，$(n-f(n))^2$能被$k^2+f(n)$整除. 因为k有无穷多个，所以，一定有$(n-f(n))^2=0$，即对于所有的$n\in\mathbf{N}_+$，有$f(n)=n$.

对于任意的素数p，由式①有

$(f(p-1)+1)\mid p^2$.

所以，$f(p-1)+1=p$或$f(p-1)+1=p^2$.

若$f(p-1)+1=p^2$，由式②知$(p^2-1)^2+1$是$[(p-1)^2+1]^2$的因数. 但由$p>1$，有

$(p^2-1)^2+1>(p-1)^2(p+1)^2$，

$$[(p-1)^2+1)]^2\leqslant[(p-1)^2+(p-1)]^2=(p-1)^2p^2,$$

矛盾. 因此，$f(p-1)+1=p$，即有无穷多个正整数 $p-1$，使得 $f(p-1)=p-1$.

第十章 裴蜀定理

1. 从两个集合中元素的表达式入手.

因为 $12m+8n+4l=4(3m+2n+l)$，

$20p+16q+12r=4(5p+4q+3r)$，

及$(3,2,1)=1$，$(5,4,3)=1$，由裴蜀定理可知

$3m+2n+l$ 与 $5p+4q+3r$ 均可表示所有整数，所以，$M=N=\{k\mid k=4l,l\in\mathbf{Z}\}$.

故选 A.

2. 将已知直线化为 $25x-15y+12=0$. 设平面上整点(x_0,y_0)到直线的距离为

$$d=\frac{|25x_0-15y_0+12|}{5\sqrt{34}}.$$

而$(25,15)=5$，由裴蜀定理知 $25x_0-15y_0$ 表示 5 的所有倍数. 当 $25x_0-15y_0=-10$ 时，d 取最小值$\frac{2}{5\sqrt{34}}=\frac{\sqrt{34}}{85}$. 故选 B.

3. $z=e^{\frac{2k\pi}{18}i}$，$w=e^{\frac{2l\pi}{48}i}$ $(k、l\in\mathbf{Z})$，则 $zw=e^{\frac{2(8k+3l)\pi}{144}i}$. 因为$(8,3)=1$，所以，$8k+3l$ 可表示所有整数，故 D 中有 144 个元素.

4. $f_n(m)=2^n(m+1)-1$. 由$(2^n,1995)=1$ 知，存在 $1\leqslant u_0\leqslant1994$，$u_0\in\mathbf{Z}$，使得 $2^nu_0+1995k_1=1$，$k_1\in\mathbf{Z}$，从而，$1995\mid(2^nu_0-1)$. 取 $m_0=u_0-1$，则 $1995\mid f_n(m_0)$，其中 $0\leqslant m_0\leqslant1993$. 唯一性可由带余除法定理证得.

5. 记 $f_{\min}=ax_0+by_0+cz_0=d_0$. 设$(a,b,c)=d$，显然有 $d\mid d_0$，从而 $d\leqslant d_0$. 另一方面，由裴蜀定理知，存在整数 x，y，z，使得 $ax+by+cz=d$. 因为 d_0 最小，故 $d_0\leqslant d$. 所以，$d_0=d$，即 $f_{\min}=(a,b,c)$.

6. 只须证 $pq-p-q$ 不可表示为 $px+qy$. 反证法. 若 $pq-p-q=ap+bq$ $(a，b$ 非负)，则 $pq=(1+a)p+(1+b)q$，因此，$p\mid(1+b)$，$q\mid(1+a)$. 令 $1+a=a'q$，$1+b=b'p\,(a',b'\geqslant1)$，得 $pq=(a'+b')pq$. 但 $a'+b'=1$，矛盾.

7. 从极端情况出发，考察球数最多和最少的盒子.

因为$(m,n)=1$，由裴蜀定理知，存在 u，$v\in\mathbf{Z}_+$，使得 $un=vm+1=v(m-1)+v+1$.

此式表明，对盒子连续加球 u 次，可使 $m-1$ 个盒子各增加 v 个球，一个盒子增加了$(v+1)$个球. 这样可将多增加了一个球的盒子选择为原来球数最少的那一个，经过 u 次加球之后，原球数最多的盒子中的球数与球数最少的盒子中的球数之差减少 1. 因此，经过有限次加球后，各盒子中的球数相等.

8. 显然，$(1,p)$和$(2,2)$满足题意.

下面考虑 $n\geqslant2$，$p\geqslant3$ 的情形.

因为$(p-1)^n+1$ 是奇数，所以，n 也是奇数. 从而，$n<2p$. 记 q 为 n 的任一素因子，则 $q\mid[(p$

$1)^n+1]$，知$(p-1)^n\equiv-1(\mathrm{mod}\ q)$，且$(q,p-1)=1$．由$q$的选取知$(n,p-1)=1$．由裴蜀定理知，存在整数$u$，$v$，使得

$un+v(q-1)=1$.

根据费尔马小定理，知

$p-1\equiv(p-1)^{un}\cdot(p-1)^{v(q-1)}\equiv(-1)^u\times1^v(\mathrm{mod}\ q)$.

因为u必为奇数，则$p-1\equiv-1(\mathrm{mod}\ q)$．这说明$q|p$，进而有$q=p$，故证得$n=p$.

于是，p^{p-1}整除$[(p-1)^p+1]=p^2(p^{p-2}-C_p^1p^{p-3}+\cdots+C_p^{p-3}p-C_p^{p-2}+1)$.

在上式的小括号中，除最后一项外均可被p整除$(p|C_p^k,1\leqslant k\leqslant p-1)$．这说明$p-1\leqslant2$，即得$p=3$.

综上所述，所有的解为$(2,2)$，$(3,3)$和$(1,p)$，其中p为任意素数.

第十一章 互素数与欧拉函数

1．首先证明$2abc-ab-bc-ca$不能表示为$xbc+yca+zab$的形式.

用反证法．设$2abc-ab-bc-ca=xbc+yca+zab$，其中$x,y,z$为非负整数，则有

$2abc=bc(x+1)+ca(y+1)+ab(z+1)$.

由归纳假设$a^{k+1}|(a+1)^b-1$.

而上式中的第二个方括号中有a个被加项，把它表示为

$[(a+1)^{(a-1)b}-1]+[(a+1)^{(a-2)b}-1]+\cdots+[(a+1)^b-1]+a$.

由(1)，即$n=0$时命题成立的结论，上式每一项都能被a整除，因而

$a|[(a+1)^{(a-1)b}+(a+1)^{(a-2)b}+\cdots+1]$.

从而有　$a^{k+2}|(a+1)^b-1$.

因此，当$n=k+1$时，命题成立．

由以上，对非负整数n，命题成立.

2．首先$x=1$，$y=1$是符合条件的一组整数解.

其次，如果(x,y)是符合条件的一组解，有$x\leqslant y$，那么考察整数对(x,y)，其中

$y^2+m=xx_1$.　①

显然，由①可知，x_1与y的任何素公约数都是m的约数，又由条件(2)，$y|x^2+m$，则这个素公约数也是x的约数.

因此有

$(x_1,y)=1$.

由①式及条件(2)可得

$x^2(x_1^2+m)=(xx_1)^2+x^2m=(y^2+m)^2+x^2m-y^4+2my^2+m(x^2+m)$是$y$的倍数.

由于$(x,y)=1$，因此$y|x_1^2+m$，从而(x_1,y)满足条件(1)，(2)，(3)，且$x_1>y\geqslant x$.

再由①式又可得(x_1,y_1)，(x_2,y_1)，(x_2,y_2)，…，且$x<x_1<x_2<\cdots$，$y<y_1<y_2<\cdots$，这一过程可无限多次进行下去，使我们得到无穷多组符合题目条件的整数.

3．取一整数m，$1\leqslant m\leqslant18$.

用连续的自然数 $n+m$，$n+m+1$，…，$n+m+13$ 这 14 个数给项链 A 的珠子标数，只要保证 $n+m$ 和 $n+m+13$ 互素，即

$$(n+m,n+m+13)=1, \quad ①$$

我们的标法就符合要求.这是因为一对相邻的整数总是互素的，又有 $n+m$ 和 $n+m+13$ 互素，则项链 A 上相邻珠子标的数都互素.

然后用 $n+m+14$ 到 $n+32(m+14\leqslant 32)$ 及 n 到 $n+m-1$ 为项链 B 的珠子标号，其条件是

$$(n,n+32)=1, \quad ②$$

和 $$(n+m-1,n+m+14)=1. \quad ③$$

由于 $(a,b)=(a,b-a)$，则①，②，③化为

$(n,32)=(n+m-1,15)=(n+m,13)=1.$

由于 n 是奇数，则 $(n,32)=1$ 自然成立.

关于 $(n+m-1,15)=1$，我们考虑以 15 为模的剩余类.

注意到 $n+m-1\not\equiv 0 \pmod{15}$，等价于

$m\not\equiv 1-n \pmod 3$，

$m\not\equiv 1-n \pmod 5$.

又由 $(n+m,13)=1$ 可知

$m\not\equiv -n \pmod{13}$.

因为在 m 的 18 个可能的数 $\{1,2,\cdots 18\}$ 中，只有 6 个满足 $m\equiv 1-n \pmod 3$，至少有 4 个满足 $m\equiv 1-n \pmod 5$，至多有 2 个满足 $m\equiv -n \pmod{13}$.

因此，至少剩下 $18-(6+4+2)=6$ 个 m 的值满足要求.

4.（1）因为 p、q 是两互异的素数，则小于 pq 且与 pq 互素的自然数，既不能被 p 整除，又不能被 q 整除.

而从 1 到 $pq-1$ 的 $pq-1$ 个自然数中，能被 p 整除的有 $q-1$ 个，能被 q 整除的有 $p-1$ 个数.

$\varphi(pq)=pq-1-(p-1)-(q-1)=(p-1)(q-1).$

(2)由(1)有

$(p-1)(q-1)=3p+q,$

$pq-4p-2q+1=0,$

$(p-2)(q-4)=7.$

$\begin{cases}p-2=1,\\q-4=7,\end{cases}$ $\begin{cases}p-2=7,\\q-4=1,\end{cases}$ $\begin{cases}p-2=-1,\\q-4=-7,\end{cases}$ $\begin{cases}p-2=-7,\\q-4=-1.\end{cases}$

解得 $p=3,q=11$.

5. 记 $\varphi(n)$ 为欧拉函数，即不超过 n 的、与 n 互素的自然数的个数.

容易看出 S_n 中每两个相邻的数互素，并且较大的数等于它左右两个相邻数的和.

下面用数学归纳法证明：在 $n\geqslant 2$ 时，每一对不大于 n 的互素数 $a>b$，在 S_2，S_3，…，S_n 中恰有两次相邻.

由对称性，因为每个 S_i 中的数都关于 2 对称，则只须证明，a 和 b 在 2 的左边恰有一次相邻.

$n=2$ 时，结论是显然的.

假设对 $n-1$ ($n-1\geqslant 2$) 结论成立.

只考虑 2 的左边.

若 $a<n$，则 a，b 在 S_n 中不相邻.

否则，若 a，b 在 S_n 中相邻，由 S_n 的构造，则 $a-b$ 与 b 均在 S_{n-1} 中并且相邻. 由归纳假设，a 和 b 在 S_2，…，S_{n-1} 中相邻，从而 $a-b$，b 在 S_2，S_3，…，S_{n-2} 中相邻. 这样，$a-b$ 和 b 在 S_2，…，S_{n-1} 中，在 2 的左边至少相邻两次，出现矛盾.

于是 a 和 b 在 S_2，…，S_n 中与在 S_2，…，S_{n-1} 中相邻的次数相同，均为一次.

若 $a=n$，则由 $n-b$，b 在 S_2，…，S_{n-1} 中仅相邻一次，所以 n，b 在 S_2，…，S_n 中仅相邻一次.

于是对 n，结论成立.

现在考虑 S_2，…，S_n（不限于 2 的左边）中那些首次出现的 n. 它们也就是 S_n 中 n 的个数，这些 n 的左邻与右邻$<n$（它们的和等于 n），并且与 n 互素.

由上面的论证，n 的左邻与右邻的个数为 $2\varphi(n)$，所以 S_n 中 n 的个数为 $\varphi(n)$.

本题的结果为：在 S_{1988} 中，1988 的个数是

$\varphi(1988)=\varphi(4)\varphi(7)\varphi(71)=840$.

6. 因为 x 是有理数，所以，x 从小数点后某位开始具有周期性. 设周期长度为 d，且设 $d=2^u v$，其中，v 是奇数，则存在正整数 w，使得 $2^w\equiv 1 \pmod v$. 特别地，可以取 $w=\varphi(v)$，其中，φ 是欧拉函数.

于是，对于每个正整数 n，有

$2^{n+w}=2^n\times 2^w\equiv 2^n \pmod v$.

又对于所有的 $n\geqslant u$，有

$2^{n+w}\equiv 2^n\equiv 0 \pmod{2^u}$.

则对于所有 $n\geqslant u$，有 $2^{n+w}\equiv 2^n \pmod d$.

因此，当 n 足够大时，x 的小数点后第 2^{n+w} 位数字与第 2^n 位数字相同. 故 y 的小数点后第 $n+w$ 位数字与第 n 位数字相同. 所以，y 小数点后的数字从某位开始以 w 为周期. 从而，y 是有理数.

7. 注意到 $k=0$ 或 $m=0$ 时，上述不定方程无解，于是，可设满足上述方程的 k，m 为正整数.

(1) 若 $k+1$ 为合数，设 $k+1=pq$，$2\leqslant p\leqslant q$，注意到，应有 $48\mid k!$. 故 $k\geqslant 6$，于是 $1<2q\leqslant k$，故 $(k+1)\mid k!$，进而 $(k+1)\mid 48$，结合 $k+1\geqslant 7$，可知 $k+1=8$，12，24 或 48，分别代入，两边约去 48 后，可得矛盾.

(2) 若 $k+1$ 为素数，由威尔逊定理，可知 $k!\equiv -1 \pmod{k+1}$，于是，$k+1\mid 47$，进而 $k+1=47$，这要求 $46!+48=48\times 47^m$. ①

从而 $m>1$，两边除以 48，可知 $\frac{46!}{48}+1=47^m$，两边模 4，可知 $(-1)^m\equiv 1 \pmod 4$，故 m 为偶数. 设 $m=2k$，则由①可知 $\frac{46!}{48}=(47^k-1)(47^k+1)$，由 $23^2\mid\frac{46!}{48}$，而 $47^k+1\equiv 2 \pmod{23}$，故 $23^2\mid 47^k-1$，利用二项式定理 $47^k=(2\times 23+1)^k\equiv 46k+1 \pmod{23^2}$，从而 $23\mid k$，进而 $m\geqslant 46$，这时，①式右边比左边大.

矛盾.

注 一般地，若 $n>4$，且 n 为合数，则 $n\mid(n-1)!$，依此可以证明威尔逊定理的逆定理也成立.

第十二章 欧拉定理、费马小定理

1. 由素数 $p\geqslant7$ 知，p 是奇数，因而 $p-1$，$p+1$，p^2+1 均为偶数，且 $p-1$ 和 $p+1$ 是相邻偶数，于是

$(p-1)(p+1)(p^2+1)=p^4-1$ 能被 $2\cdot2\cdot4=16$ 整除.

又由费马小定理，$(p,3)=1$，$(p,5)=1$，则

$3\mid p^2-1$，$5\mid p^4-1$.

因为 16，3 和 5 两两互素，则

$16\cdot3\cdot5\mid p^4-1$，即 $240\mid p^4-1$.

2. 设 p 为素数，由费马小定理知

$2^{p-1}\equiv1\pmod p$.

设 n 与 $p-1$ 的最大公约数为 d.

如果 $n>1$，且 $2^n\equiv1\pmod p$，则

$2^d\equiv1\pmod p$.

从而 n 的最小素因数 $m(n)\leqslant d\leqslant p-1<p$.

假设结论不成立，即 $n_1,n_2,\cdots,n_k$ 中有大于 1 的，如 $n_1>1$，那么 $n_k>1,n_{k-1}>1,\cdots,n_2>1$.

由于 $n_2\ 2^{n_1}-1$，则

$m(n_2)\mid2^{n_1}-1$.

从而有 $m(n_2)>m(n_1)$.

同理有 $m(n_2)<m(n_3)<\cdots<m(n_1)$.

出现矛盾.

所以 $n_1=n_2=\cdots=n_k=1$.

3. 如果 m 和 n 都是偶数，则 3^m+1 能被 4 整除．但这是不可能的，因为对所有的偶数 m，$3^m+1\equiv2\pmod 4$，故 m，n 中至少有一个是奇数.

不妨设 m 为奇数，且 $m\neq1$，设 p 为整除 m 的最小素数，且 $m=pk$，易知 $p\geqslant5$.

由费马小定理有

$3^{p-1}\equiv1(\mathrm{mod}\ p)$.

由题设有

$3^{2pk}\equiv1(\mathrm{mod}\ p)$.

由素数 p 的定义有 $(2pk,\ p-1)=2$，所以，

$3^2\equiv1(\mathrm{mod}\ p)$.

这是不可能的，因此，m 和 n 中至少有一个等于 1．这意味着满足条件的 $(m,\ n)$ 为

$(1,\ 1)$，$(1,\ 2)$，$(2,\ 1)$.

4. 因为 $p-1$ 是偶数，故

$$\sum_{k=1}^{p-1}k^{2p-1}=\sum_{k=1}^{\frac{p-1}{2}}[k^{2p-1}+(p-k)^{2p-1}].$$

由二项式定理，得

$(p-k)^{2p-1}=p^{2p-1}-\cdots-C_{2p-1}^{2}p^{2}k^{2p-3}+C_{2p-1}^{1}pk^{2p-2}-k^{2p-1}$.

故 $k^{2p-1}+(p-k)^{2p-1}\equiv k^{2p-1}+C_{2p-1}^{1}pk^{2p-2}-k^{2p-1}=(2p-1)pk^{2p-2}\pmod{p^2}$.

对 $1\leqslant k\leqslant p-1$，必有 $(k,p)=1$.

由费马小定理，得 $k^{p-1}\equiv1\pmod p$.

故 $(2p-1)k^{2p-2}\equiv(2p-1)\times1^2\equiv-1\pmod p$.

从而，$(2p-1)pk^{2p-2}\equiv-p\pmod{p^2}$，因此，

$$\sum_{k=1}^{p-1}k^{2p-1}\equiv-p\cdot\frac{p-1}{2}\equiv\frac{p-p^2}{2}+p^2\equiv\frac{p(p+1)}{2}\pmod{p^2}.$$

5. 先证明一个引理.

引理　若 p 为素数，则 2^p-1 也是素数.

引理的证明　反证法.

假设存在素数 q $(q>2)$，使得 $q\mid(2^p-1)$，即

$2^p\equiv1\pmod q$.

由费马小定理知

$2^{q-1}\equiv1\pmod q$，

故存在最小的正整数 $r_0>1$，使得

$2^{r_0}\equiv1\pmod q$.

设 $p=kr_0+r$，$0\leqslant r<r_0$，则

$2^p=2^{kr_0+r}=2^{kr_0}\times2^r\equiv2^r\equiv1\pmod q$.

故 $r=0$，$r_0\mid p$. 矛盾.

下面证明原题.

有无限多个素数 p，满足 $W(p)\mid(2^p-1)$，有三种可能情况.

(1) 有无限多个 p，使得 $W(p)=1$，则 $W(x)=1$；

(2) 有无限多个 p，使得 $W(p)=-1$，则 $W(x)=-1$；

(3) 有无限多个 p，使得 $|W(p)|=2^p-1$. 设 $W(x)$ 最高次项为 ax^n，则当 p 充分大时，$|W(p)|<2ap^n<2^p-1$. 矛盾.

故 $W(x)=1$ 或 $W(x)=-1$.

6. 对任意 $y\in\{0,1,\cdots,2005\}$，当 y 能被 2,3,5 整除时，就有 $f(y)=f(y+1)$ 成立.

对于一个变量 y，要使得 $f(y)$ 和 $f(y+1)$ 不相等，则 $(y,30)=1$. 因为 $\varphi(30)=8$，$2005=30\times66+25$，故 $\{0,1,\cdots,2005\}$ 中与 30 互素的数有

$66\times8+7=535$（个）.

其将 $\{0,1,\cdots,2005\}$ 分成 536 个部分，每一部分的函数值相等.

综上所述，函数 f 的最多取值有 536 个.

7. 如果存在自然数 N，使得 $a_{N+1},a_{N+2},\cdots$ 是周期数列. 设其周期为 T，令

$T=2^{\alpha_1}\cdot 5^{\alpha_2}\cdot p$，其中 α_1,α_2 为非负整数，且 $(p,10)=1$.

取自然数 $m\geqslant\max\{\alpha_1,\alpha_2\}$，且 $10^m>N$.

取 $k=m+\varphi(p)$，其中 $\varphi(p)$ 表示 $[1,p]$ 中与 p 互素的整数的个数.

由欧拉定理可知

$10^{\varphi(p)}-1\equiv 0 \pmod p$.

所以有 $10^m(10^{\varphi(p)}-1)\equiv 0 \pmod T$，即 $10^k\equiv 10^m \pmod T$.

由于 $(10^k)!=10^k(10^k-1)!$，从而由 a_n 的定义可知

$a_{10^k}=a_{10^k-1}$.

显然 $10^k-1>N$，于是

$a_{2\cdot 10^k-10^m}=a_{2\cdot 10^k-10^m-1}$.

显然，$2\cdot 10^k-10^m$ 的第一个非零数字是 9，又

$(2\cdot 10^k-10^m)!=(2\cdot 10^k-10^m)(2\cdot 10^k-10^m-1)!$，

所以 $a_{2\cdot 10^k-10^m-1}=5$.

但这是不可能的. 这是因为在 $n!=2^{\alpha_2}\cdot 3^{\alpha_3}\cdot 5^{\alpha_5}\cdots$ 的素因子分解中，满足

$$\alpha_2=\sum_{k=1}^{\infty}\left[\frac{n}{2^k}\right]\geqslant\alpha_5=\sum_{k=1}^{\infty}\left[\frac{n}{5^k}\right].$$

即 $n!$ 中 2 的最高指数不小于 5 的最高指数.

所以使 a_{N+1}，a_{N+2}，…为周期数列的 N 不存在.

8. 假设对于某个 $n>1$ 的整数，使得 $n\mid 2^n-1$，则 n 必为奇数.

设 p 为 n 的最小素因数（n 为素数时，$p=n$）.

由欧拉定理可知

$2^{\varphi(p)}=2^{p-1}\equiv 1 \pmod p$. ①

令整数 q 满足不等式 $0<n-(p-1)q<p-1$，则

$q=\left[\frac{n}{p-1}\right]$.

对①应用同余式的性质可得

$2^{q(p-1)}\equiv 1 \pmod p$. ②

又由 $n\mid 2^n-1$ 得

$2^n\equiv 1 \pmod p$. ③

记 $\lambda_1=n-(p-1)q$.

对②，③应用同余式性质可得

$2^{\lambda_1}\equiv 1 \pmod p$. ④

因为 $0<\lambda_1<p-1$，所以 $\lambda_1\nmid p$，进而 $\lambda_1\nmid n$.

令 $n=q_1\lambda_1+\lambda_2$，其中 q_1 为整数，且 $0<\lambda_2<\lambda_1$.

由③，④应用同余式性质可得

$2^{\lambda_2}\equiv 1 \pmod p$.

依此类推，可求得一系列同余式

$2^{\lambda_k}\equiv 1 \pmod p$，$k=1$，$2\cdots$，$t$.　⑤

其中 λ_k 满足 $\lambda_1>\lambda_2>\cdots>\lambda_t>0$.

由于 $(n, p-1)=1$，由无限递降的结果，最后必有 $\lambda_1=1$.

这时⑤式化为 $2\equiv 1 \pmod p$，这是不可能的.

因此 $n\nmid 2^n-1$.

9. 令 $f(n)=g(n)+1$,则

$f(1)=1, f(2)=2$,　①

$f(n+2)=f(n)+f(n+1)$.　②

则 $\{f(n)\}$ 为斐波那契数列,由①,②可知

$$f(n)=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}}.\qquad ③$$

当 n 为大于 5 的素数时,由费马小定理

$5^{n-1}\equiv 1 \pmod n$.

因为 n 为奇素数,则 $\frac{n-1}{2}$ 为整数,于是

$n\mid 5^{n-1}-1=(5^{\frac{n-1}{2}}+1)(5^{\frac{n-1}{2}}-1)$.　④

若 $n\mid(5^{\frac{n-1}{2}}+1)$,则由于 $0<j<n$ 时,

$n\mid C_n^j$.

$$2^n f(n)=\frac{(\sqrt{5}+1)^{n+1}-(1-\sqrt{5})^{n+1}}{2\sqrt{5}}=\frac{(\sqrt{5}+1)^n-(1-\sqrt{5})^n}{2}+\frac{(\sqrt{5}+1)^n+(1-\sqrt{5})^n}{2\sqrt{5}}$$

$$=\sum_{k=0}^{\frac{n-1}{2}}C_n^{2k}(\sqrt{5})^{2k}+\sum_{k=0}^{\frac{n-1}{2}}C_n^{2k+1}(\sqrt{5})^{2k}\equiv 1+5^{\frac{n-1}{2}}\equiv 0 \pmod n.$$

若 $n\nmid(5^{\frac{n-1}{2}}+1)$,则由④

$n\mid(5^{\frac{n-1}{2}}-1)$.

所以有　$2^n(f(n)-1)\equiv 1+5^{\frac{n-1}{2}}-2^n\equiv 2-2^n\equiv 0 \pmod n$.

最后一步是因为由欧拉定理

$2^{n-1}\equiv 1 \pmod n$,

$2^n\equiv 2 \pmod n$,

$2^n-2\equiv 0 \pmod n$.

由以上,总有 $n\mid 2^n f(n)(f(n)-1)$.

因为 $(2,n)=1$,则 $n\mid f(n)(f(n)-1)$,即

$n\mid g(n)(g(n)+1)$.

10. 设 $\varphi(m)$ 为欧拉函数,即 $\varphi(m)$ 表示小于所给正整数 m,且与 m 互素的正整数的个数.

在大于 1 的自然数 n 中,我们按如下方法选出一个无穷子列:

(1) 取 $n_0=3$,

取 $n_1=\varphi(2^{n_0}-3)=\varphi(5)=4$.

(2) 若 n_k 已取出，则取

$n_{k+1}=\varphi(2^{n_0}-3)\varphi(2^{n_1}-3)\cdots\varphi(2^{n_k}-3)=n_k\cdot\varphi(2^{n_k}-3)$, $(k\geqslant 1)$.

这样,我们给出了数列$\{2^n-3\}$的一个无穷子列 $2^{n_0}-3,2^{n_1}-3,2^{n_2}-3,\cdots$.

现在只要能够证明

$(2^{n_{k+1}}-3,2^{n_i}-3)=1$,其中 $i=0,1,2,\cdots,k$.

那么这个无穷子列就符合题设要求.

为此要用到欧拉-费马定理:

若 a 与 m 互素,则

$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m)$.

取 $a=2,m=2^n-3\ (n=3,4,5,\cdots)$,则上式成立.

于是有 $\quad 2^{\varphi(2^{n_i}-3)}\equiv 1\ (\mathrm{mod}\ (2^{n_i}-3))$,

$2^{n_{k+1}}=[2^{\varphi(2^{n_i}-3)}]^{\varphi(2^{n_0}-3)\varphi(2^{n_1}-3)\cdots\varphi(2^{n_{i-1}}-3)\varphi(2^{n_{i+1}}-3)\cdots\varphi(2^{n_k}-3)}\equiv 1\ (\mathrm{mod}\ (2^{n_i}-3))$.

所以有 $\quad 2^{n_{k+1}}-3\equiv -2\ (\mathrm{mod}\ (2^{n_i}-3))$.

此时,若 t 是 $2^{n_{k+1}}-3$ 和 $2^{n_i}-3$ 的一个公因子,则有 $t|2$.

又因为 $2\nmid 2^{n_i}-3$,则 $t\neq 2$,即 $t=1$.

即证得$(2^{n_{k+1}}-3,2^{n_i}-3)=1$,$(i=0,1,2,\cdots,k)$成立.

所以无穷子列$\{2^{n_i}-3\}(i=0,1,2,\cdots)$中的项两两互素.

11. 显然，$b\geqslant 2$.

假设$\dfrac{b^n-1}{b-1}=p^l$ (p 为素数).

则当 $n\geqslant 2$ 时，$l\geqslant 1$.

若 $n=xy$，其中，x，y 均大于 1，则

$\dfrac{b^{xy}-1}{b-1}=\dfrac{b^{xy}-1}{b^y-1}\cdot\dfrac{b^y-1}{b-1}=(1+b^y+\cdots+b^{y(x-1)})\dfrac{b^y-1}{b-1}$.

因为$\dfrac{b^{xy}-1}{b-1}=p^l$，且 $x>1$，$y>1$，所以，$\dfrac{b^{xy}-1}{b-1}$的每一个因数均为 p 的幂.

因此,$p|(b^y-1)$,即

$b^y\equiv 1(\mathrm{mod}\ p)$.

所以,$1+b^y+\cdots+b^{y(x-1)}\equiv x(\mathrm{mod}\ p)$.

于是,$p|x$.

又 x 为 n 的任意大于 1 的因数,故由上述分析过程知 $n=p^m(m\in\mathbf{N}_+)$,因此,

$\dfrac{b^{p^m}-1}{b-1}=\dfrac{b^{p^m}-1}{b^{p^{m-1}}-1}\cdot\cdots\cdot\dfrac{b^{p^2}-1}{b^p-1}\cdot\dfrac{b^p-1}{b-1}$,

其中,每一个因数均是 p 的幂,且均大于 1.

从而,$p|(b^p-1)$,即 $b^p\equiv 1(\mathrm{mod}\ p)$.

又由费马小定理知

$b^p\equiv b(\bmod p)$.

因此，$b\equiv1(\bmod p)$，故 $p\mid(b-1)$.

又由 $p\left|\dfrac{b^p-1}{b-1}\right.$，得

$p^2\mid(b^p-1)$，即 $b^p\equiv1(\bmod p^2)$.

若 $m\geqslant2$，考虑

$$\frac{b^{p^2}-1}{b^p-1}=1+b^p+\cdots+b^{p(p-1)}. \qquad ①$$

一方面，易知式①右端模 p^2 余 p.

另一方面，由式①右端知其大于 p，故其必被 p^2 整除．矛盾.

因此，$m=1$，即 n 必为素数.

12．由 $n-1$ 个 1 和 1 个 7 组成的自然数 N 可表示为

$N=A_n+6\cdot10^k$，其中 A_n 是由 n 个 1 组成的自然数，$0\leqslant k\leqslant n$.

当 $3\mid n$ 时，A_n 的各数码之和可被 3 整除，所以

$3\mid A_n$.

从而　$3\mid N$.

又因为 $N>3$，所以 N 不是素数.

现考虑 $3\nmid n$ 的情况.

由费马小定理得

$(10^6)^t\equiv1(\bmod 7)$，

$10^{6t}\equiv1(\bmod 7)$.

于是　$A_{6t+s}\equiv A_{6t}+A_s\cdot10^{6t}\equiv A_{6t}+A_s\quad(\bmod 7)$.

注意到

$10^0\equiv1\ (\bmod 7)$，$10^1\equiv3\ (\bmod 7)$，$10^2\equiv2\ (\bmod 7)$，

$10^3\equiv6\ (\bmod 7)$，$10^4\equiv4\ (\bmod 7)$，$10^5\equiv5\ (\bmod 7)$.

又因为

$A_1\equiv1\ (\bmod 7)$，$A_2\equiv4\ (\bmod 7)$，$A_3\equiv6\ (\bmod 7)$，

$A_4\equiv5\ (\bmod 7)$，$A_5\equiv2\ (\bmod 7)$，$A_6\equiv0\ (\bmod 7)$，

所以，当且仅当 $6\mid n$ 时，

$A_n\equiv0\ (\bmod 7)$.

于是，$6\nmid n$ 时，

$A_n\equiv r\neq0\ (\bmod 7)$.

因此，当 $6\nmid n$ 时，必存在一个 k，$0<k\leqslant5$，使得 $6\cdot10^k\equiv7-r\ (\bmod 7)$.

从而，当 $6\nmid n$，且 $n>6$ 时有

$N=A_n+6\cdot10^k\equiv r+(7-r)\equiv0\ (\bmod 7)$.

此时，N 不是素数.

最后考虑 $n=1$，2，4，5 时的情形.

$n=1$ 时，$N=7$ 是素数；

$n=2$ 时，$N=17$，71 是素数；

$n=4$ 时，有 $1711=29\cdot59$ 不是素数；

$n=5$ 时，有 $11711=11111+6\cdot10^2\equiv0\pmod 7$，即 $11711=7\cdot1673$ 不是素数.

所以满足本题要求的只有 $n=1$，2.

13. 先证明如下的引理.

引理：当 a 历遍模 2^{1999} 的一个简化剩余系时，a^{19} 亦历遍模 2^{1999} 的一个简化剩余系.

事实上，由于当 $(a,2^{1999})=1$ 时，$(a^{19},2^{1999})=1$. 故引理只需要证明当 $a\not\equiv b\pmod{2^{1999}}$ 且 a,b 均为奇数时，$a^{19}\not\equiv b^{19}\pmod{2^{1999}}$.

有两种截然不同的做法证明这一论断. 一种是设 $a\equiv bc\pmod{2^{1999}}$，$c$ 为奇数，反设 $a^{19}\equiv b^{19}\pmod{2^{1999}}$，则 $c^{19}\equiv1\pmod{2^{1999}}$. 设 l 为 c 对模 2^{1999} 的阶，则 $l\mid19$，且 $l\mid\varphi(2^{1999})$ [因为 $c^{\varphi(2^{1999})}\equiv1\pmod{2^{1999}}$，欧拉定理]，故可知 $l\mid(19,\varphi(2^{1999}))$，所以

$l=1$，$c\equiv1\pmod{2^{1999}}$，

故 $a\equiv b\pmod{2^{1999}}$，矛盾.

另一种证法是因式分解. 由于 $(a^{19}-b^{19})=(a-b)(a^{18}+a^{17}b^1+\cdots+ab^{17}+b^{18})$，而 $a^{18}+a^{17}b+\cdots+ab^{17}+b^{18}$ 为 19 个奇数之和仍为奇数，故

$2^{1999}\mid a^{19}-b^{19}\Leftrightarrow2^{1999}\mid a-b$.

下证原命题.

由于 $2m-1$ 与 2^{1999} 互素，故由引理，可知存在 $a\in\mathbf{Z}$，$(a,2^{1999})=1$，且 $a^{19}\equiv2m-1\pmod{2^{1999}}$. 不妨设 $a^{19}<2m-1$，否则我们可以取充分大的 $t\in\mathbf{Z}^+$，用 $a-t\cdot2^{1999}$ 代替上面的 a. 故可设 $k\in\mathbf{Z}$，使 $2m-1=a^{19}+k\cdot2^{1999}$.

由于 $a^{19}<2m-1$，故 $k\in\mathbf{Z}^+$.

故我们找到了这样的 3 个整数 a，1，k，其中 a，1 均为奇数，$k>0$，使

$2m=a^{19}+1^{99}+k\cdot2^{1999}$.

从而原命题得证.

14. 首先我们证明 S 中的每一个数均与 mn 互素.

依题意 $(m,n)=1$，$(b_i,n)=1$，$i=1,2,\cdots,s$，所以

$(mb_i+na_j,n)=(mb_i,n)=1$.

同理 $(mb_i+na_j,m)=1$，从而 S 中每个数均与 mn 互素.

其次我们证明 S 中每两个数对模 mn 不同余.

设有 $mb_i+na_j\equiv mb'_i+na'_j\pmod{mn}$，则

$mb_i\equiv mb'_i\pmod{mn}$.

又 $(m,n)=1$，所以 $b_i\equiv b'_i\pmod n$，即 $b_i=b'_i$.

同理 $a_j=a'_j$，从而 $mb_i+na_j=mb'_i+na'_j$.

最后证明任一与 mn 互素的数 C 必与 S 的某个元素在模 mn 的同一个剩余类中.

由裴蜀定理知存在整数 u,v 使得 $mu+nv=C$. 因为 $(m,n)=1$，$(C,n)=1$，所以 $(u,n)=(mu,n)=(C-nv,n)=(C,n)=1$.

同理$(v,n)=1$. 从而依题意可知分别存在b_i,a_j，使得$b_i\equiv u \pmod n$，$a_j\equiv v \pmod m$，即有$mb_i+na_j\equiv C \pmod{mn}$.

综上所述，S确实是模mn的缩系.

注 由于$t=\varphi(m)$，$s=\varphi(n)$，$\operatorname{card}(s)=st=\varphi(mn)$，从而在$(m,n)=1$时，有$\varphi(mn)=\varphi(m)\varphi(n)$. 由此可导出欧拉函数的表达式. 事实上，当$p$为素数，$\alpha$为正整数时，在$0,1,2,\cdots,p^\alpha-1$中共有$0,p,\cdots,p(p^{\alpha-1}-1)$这$p^{\alpha-1}$个数是$p$的倍数，其余的均与$p^\alpha$互素. 从而$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}=p^\alpha\left(1-\frac{1}{p}\right)$.

由上面两个式子即可得到$\varphi(n)$的计算公式：

设n的分解式为$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$.

15. 由$(a,p_1p_2\cdots p_k)=1$，有$(a,p_1)=1$. 由费马小定理，$a^{p_1-1}\equiv1 \pmod{p_1}$，又$k\geqslant2$，$p_2,\cdots,p_k$为奇素数，则$\frac{(p_2-1)\cdots(p_k-1)}{2}$为正整数，从而$a^{(p_1-1)(p_2-1)\cdots(p_k-1)}\equiv1 \pmod{p_1}$，即

$$p_1\mid a^{(p_1-1)\cdots(p_k-1)/2}-1.$$

同理，$a^{(p_1-1)\cdots(p_k-1)/2}-1$能被$p_1,p_2,\cdots,p_k$整除.

从而$a^{\frac{1}{2}(p_1-1)\cdots(p_k-1)}+1$不能被$p_1,p_2,\cdots,p_k$整除.

注意到$\frac{(p_1-1)\cdots(p_k-1)}{2}$是一个偶数，则

$$a^{(p_1-1)\cdots(p_k-1)/2}\equiv0\text{ 或 }1 \pmod 4,$$

因此，4不整除$a^{(p_1-1)\cdots(p_k-1)/2}+1$，故它有异于$p_1,p_2,\cdots,p_k$的奇素因数. 所以

$$a^{(p_1-1)\cdots(p_k-1)}-1=[a^{(p_1-1)\cdots(p_k-1)/2}-1][a^{(p_1-1)\cdots(p_k-1)/2}+1]$$

有异于$p_1,p_2,\cdots,p_k$的奇素因数.

16. (1) 设p为素数，由$p\mid a^p-1$，可知$(a,p)=1$，于是由费马小定理可知$a^{p-1}\equiv1 \pmod p$，而$a^p-1=a(a^{p-1}-1)+(a-1)$，故$a\equiv1 \pmod p$，因此$a^i\equiv1 \pmod p$，$i=0,1,2,\cdots,p-1$. 将上述p个同余式求和，得

$$A=a^{p-1}+a^{p-2}+\cdots+a+1\equiv p\equiv0 \pmod p.$$

于是$p^2\mid a^p-1$，从而p具有性质P.

(2) 设p为奇素数，我们证明：$2p$具有性质P.

事实上，由$2p\mid a^{2p}-1$，可知a为奇数，从而$a^{2p}=(a^p)^2\equiv1 \pmod 8$，故$4\mid a^{2p}-1$.

另一方面，$p\mid a^{2p}-1$，故$p\mid(a^p-1)(a^p+1)$，从而，$p\mid a^p-1$或$p\mid a^p+1$. 若$p\mid a^p-1$，则由前面(1)的结论，可知$p^2\mid a^p-1$；若$p\mid a^p+1$，则$(a,p)=1$，利用费马小定理，可知$a^{p-1}\equiv1 \pmod p$，进而$-1\equiv a^p\equiv a \pmod p$，即$p\mid a+1$. 注意到$p$为奇数，于是$B=a^{p-1}-a^{p-2}+\cdots+1\equiv(-1)^{p-1}-(-1)^{p-2}+\cdots+1=p\equiv0 \pmod p$，从而$p^2\mid a^p+1$. 所以总有$p^2\mid a^{2p}-1$.

结合$(4,p^2)=1$，可知$4p^2\mid a^{2p}-1$，于是$2p$具有性质P. 由素数有无穷多个，可知(2)成立.

17. 由条件$p^\alpha\mid a^p-1$，于是$p\mid a^p-1$，故$(a,p)=1$，由费马小定理可知$a^{p-1}\equiv1 \pmod p$，所以$a^{p-1}\equiv1\equiv a^p \pmod p$，故$a\equiv1 \pmod p$.

另一方面，设$A=a^{p-1}+a^{p-2}+\cdots+1$，则$a^p-1=(a-1)A$，且$A\equiv1^{p-1}+1^{p-2}+\cdots+1=p\equiv$

$0\pmod p$，即 $p\ A$. 进一步，设 $a=kp+1$，由二项式定理，可知

$$A\equiv kp[(p-1)+(p-2)+\cdots+1]+p=\frac{(p-1)k}{2}\cdot p^2+p\equiv p\pmod{p^2}.$$

最后一步用到 p 为奇素数. 所以 $p\parallel A$（说明：一般地，若 $p^\alpha|A$，而 $p^{\alpha+1}\nmid A$，则记 $p^\alpha\parallel A$）.

综上所述，结合 $p^\alpha|(a^p-1)$，可知 $p^{\alpha+1}|a-1$. 命题获证.

当 $p=2$ 时，命题不成立，例如 $2^3|3^2-1$，但是 $2\nmid 3-1$.

18. 由于 $\frac{p^p-1}{p-1}=1+p+p^2+\cdots+p^{p-1}\equiv p+1\pmod{p^2}$，则

$\frac{p^p-1}{p-1}$ 中至少有一个素因子 q，满足 $q\not\equiv 1\pmod{p^2}$.

下面证明 q 为所求.

假设存在整数 n，使得 $n^p\equiv p\pmod q$，则由 q 的选取，有 $n^{p^2}\equiv p^p\equiv 1\pmod q$.

另一方面，由费马小定理，有 $n^{q-1}\equiv 1\pmod q$ [由于 q 为素数且 $(n,q)=1$].

由于 $p^2\nmid(q-1)$，有 $(p^2,q-1)|p$，因此，

$n^p\equiv 1\pmod q$，从而 $p\equiv 1\pmod q$，则导出 $1+p+\cdots+p^{p-1}\equiv p\pmod q$.

由 q 的选取，有 $p\equiv 0\pmod q$，矛盾. 所以，命题成立.

19. 当 $p=2$ 时，只有整数 $n=1,2$ 满足要求. 下面考虑 p 为不小于 3 的奇素数的情形. 这时候，$(p-1)^n+1$ 为奇数，故 n 只可能为奇数[因为 n 为 $(p-1)^n+1$ 的因子]，先设 $n>1$.

设 n 的最小素因数为 $q\geqslant 3$，则 n 可以表示成 $n=q^k\cdot s$，其中 $k\geqslant 1$，且 $q\nmid s$，s 为奇数($\geqslant 1$)，且 s 的每个素因数(如果 $s\neq 1$ 的话)均大于 q.

于是由 $(p-1)^n\equiv -1\pmod{n^{p-1}}$ 可知 $(p-1)^n\equiv -1\pmod q$，再根据费马小定理(注意 $p-1$ 与 q 互素)，$(p-1)^{q^k}\equiv p-1\pmod q$.

∴ $(p-1)^s\equiv -1\pmod q$.

设 l 为 $p-1$ 对模 q 的阶，则 $(p-1)^l\equiv 1\pmod q$.

我们又有如下三个关系式：

$(p-1)^s\equiv -1\pmod q$，$(p-1)^{2s}\equiv 1\pmod q$，$(p-1)^{q-1}\equiv 1\pmod q$.

可知

$l|2s$，$l|q-1$，$l\nmid s$，∴ l 为偶数且 $l|(2s,q-1)$.

由 q 及 s 的取法，∴ $(2s,q-1)=2$.

故 $l=2$. ∴ $(p-1)^2\equiv 1\pmod q$.

而 $p-1\not\equiv 1\pmod q$，只可能是 $p-1\equiv -1\pmod q$，∴ $q=p$.

故 $p|n$. 又 $n\leqslant 2p$，从而 $n=p$.

题目条件化为 $(p-1)^p\equiv -1\pmod{p^{p-1}}$.

若 $p\geqslant 5$，故 $p^3|p^{p-1}$.

∴ $(p-1)^p+1$ 能被 p^3 整除.

$$但(p-1)^p+1=\sum_{j=3}^{p}C_p^j\cdot(-1)^{p-j}\cdot p^j+C_p^2\cdot(-1)^{p-2}\cdot p^2+p^2.$$

它除了最后一项 p^2 外每一项均被 p^3 整除，矛盾.

故 p 只能等于 3. 所求的 $(n,p)=(3,3)$，还有 $n-1$ 的平凡情形满足要求. 故所求的一切解 (n,p) 为 $(2,2)(3,3)(1,p)$（p 为任意素数）.

第十三章　中国剩余定理

1. 设 $m=11^i p$，$n=11^j q$，其中 i，j 为非负整数，且 $11\nmid p$，$11\nmid q$.

为证明存在某个整数 l，使得 $m=11^l n$，只需证明 $p=q$.

设 $p>q$（$p<q$ 的情形可仿此讨论）.

因为 $(p,11)=1$，所以由中国剩余定理，存在正整数 a，使得

$a\equiv 0 \pmod p$，

$a\equiv -1 \pmod{11}$，

于是　$a=11k-1(k\in \mathbf{N})$.

$(11^k-1,m)=(a,11^i p)=p$，

$(11^k-1,n)=(a,11^j q)\leqslant q<p$.

此时与已知条件 $(11^k-1,m)=(11^k-1,n)$ 矛盾.

于是 $p=q$，即 $m=11^{i-j}n$.

2. 用反证法.

假定能找到整数 x_1，x_2，…，x_m，使得对任何 $k=1$，2，…，m，函数值 $F(x_k)$ 都不是 a_k 的倍数.

这就意味着，存在着整数 $d_k=p_k^{\alpha_k}$，使得 a_k 可被 d_k 整除，但 $F(x_k)$ 却不能被 d_k 整除.

如果在 d_1，d_2，…，d_m 中存在有同一个素数的方幂，则可仅留下其中幂次最低的，去掉那些幂次较高的，因为如果 $F(x)$ 不能被幂次最低者整除，那么当然就更不能被幂次更高的整除.

这样一来，可以得到一个两两互素的数组 d_1，d_2，…，d_s，由中国剩余定理知，存在整数 N，使得

$N\equiv x_k \pmod{d_k}, k=1,2,\cdots,s.$

从而 $F(N)$ 不可被 d_k 中任何一个整除，因此也不可被 a_k 中的任何一个整除，与题意矛盾.

3. 结论是正确的.

(1) 设 $ad-bc$ 的每个素约数都是 a 和 c 的约数，但存在某个整数 n，$an+b$ 与 $cn+d$ 不互素.

这时，$an+b$ 与 $cn+d$ 对某个 n，能被某个素数 p 整除，于是由

$ad-bc=a(cn+d)-c(an+b)$，

$ad-bc$ 能被素数 p 整除，所以 a 与 c 也能被 p 整除. 因此

$b=(an+b)-an$，$d=(cn+d)-cn$

也能被 p 整除，从而 a，b，c，d 的最大公约数不小于 p，与题设的 a，b，c，d 的最大公约数等于 1 矛盾.

因此，对每个 n，$an+b$ 与 $cn+d$ 都互素.

(2) 设对某个整数 n，$an+b$ 与 $cn+d$ 互素，但对 $ad-bc$ 的某个素约数 p 不是 a 的约数，即

$ad-bc\equiv 0 \pmod p$，

　　$a\not\equiv 0 \pmod p$.

[对 $c\not\equiv 0\ (\text{mod}\ p)$可仿此讨论.]

则由中国剩余定理,存在整数 n,使得

$an\equiv -b\ (\text{mod}\ p)$,即 $an+b\equiv 0(\text{mod}\ p)$.

$a(cn+d)=c(an+b)+(ad-bc)\equiv 0\ (\text{mod}\ p)$.

因为$(a,p)=1$,所以

$cn+d\equiv 0\ (\text{mod}\ p)$.

此时$(an+b,cn+d)\geqslant p>1$,出现矛盾.

因此,$ad-bc$ 的任何素约数都是a 与c 的约数.

4. 任取自然数 a_1,设已有自然数集合

$S'=\{a_1,a_2,\cdots,a_n\}$,

且 S'中任意两数互素,任意 $k(2\leqslant k\leqslant n)$个数的和为合数.

取 2^n-1 个与乘积 $a_1a_2\cdots a_n$ 互素的素数 $P_j\,(1\leqslant j\leqslant 2^n-1)$.

设由 $a_1,a_2,\cdots,a_n$ 每次取 k 个$(1\leqslant k\leqslant n)$所得的

$C_n^1+C_n^2+\cdots+C_n^n=2^n-1$

个和为 $S_j\,(1\leqslant j\leqslant 2^n-1)$.

考虑同余方程组

$$\begin{cases}a_1a_2\cdots a_nx+1+S_1\equiv 0\ (\text{mod}\ p_1^2),\\ a_1a_2\cdots a_nx+1+S_2\equiv 0\ (\text{mod}\ p_2^2),\\ \cdots\cdots\\ a_1a_2\cdots a_nx+1+S_{2^n-1}\equiv 0\ (\text{mod}\ p_{2^n-1}^2).\end{cases}$$

由中国剩余定理,这个方程组必有正整数解 x,令 $a_{n+1}=a_1a_2\cdots a_nx+1$,则

a_1,a_2,$\cdots$,a_n,a_{n+1}两两互素,且任意 k 个 $(2\leqslant k\leqslant n+1)$ 的数的和为合数.

这样,我们就由 n 个元素的集合 S'生成一个新元素 a_{n+1}得到 $n+1$ 个元素的 S'',而 S''符合题目要求.

于是,我们可以找到含有 1990 个自然数且符合题目要求的集合 S.

5. 证法 1 对 n 进行归纳. 当 $n=1$ 时显然,取 $k_0=3$,$k_1=7$ 即可.

假设对给定的 n,存在两两互素的整数 $1<k_0<k_1<\cdots<k_n$ 及正整数 a_n 使得 $k_0k_1\cdots k_n-1=a_n(a_n-1)$. 取 $k_{n+1}=a_n^2+a_n+1$,则

$k_0k_1\cdots k_{n+1}=(a_n^2-a_n+1)(a_n^2+a_n+1)=a_n^4+a_n^2+1$,

所以 $k_0k_1\cdots k_{n+1}-1$ 是两个连续整数 a_n^2 和a_n^2+1 的乘积,而且

$\gcd(k_0k_1\cdots k_n,k_{n+1})=\gcd(a_n^2-a_n+1,a_n^2+a_n+1)=1$,

因此 $k_0,k_1,\cdots,k_{n+1}$两两互素. 证毕.

证法 2 我们只需证明:对任意正整数 n,存在正整数 x,使得 x^2+x+1 至少含有 n 个不同的素因子.

下面证明更一般的结论.

命题:设 $P(x)=a_dx^d+\cdots+a_1x+1$ 为整系数多项式,$d\geqslant 1$,则对任意正整数 n,存在正整数 x,使得 $P(x)$至少含有 n 个不同的素因子.

命题的证明由下面两个引理给出.

引理1 集合 $Q=\{p \mid p$ 是素数，存在整数 x，使得 p 整除 $P(x)\}$ 是无限集.

证明：假设集合 Q 仅存在有限个素数 $p_1, p_2, \cdots, p_k$，则对任一整数 m，$P(mp_1p_2\cdots p_k)$ 是个不存在素因子的整数,因此 $P(mp_1p_2\cdots p_k)$ 等于1或 -1.然而 $P(x)$ 为 d 次多项式,故 $P(x)$ 最多出现 d 个1和 d 个 -1. 矛盾.

引理2 设 $p_1, p_2, \cdots, p_n (n\geqslant 1)$ 为属于集合 Q 的 n 个素数,则存在正整数 x,使得 $P(x)$ 被 $p_1p_2\cdots p_n$ 整除.

证明:对于 $i=1,2,\cdots,n$,因为 $p_i\in Q$,所以存在 c_i,使得 $P(x)$ 被 p_i 整除,其中 $x\equiv c_i \pmod{p_i}$. 根据中国剩余定理，一次同余方程组 $x\equiv c_i \pmod{p_i}, i=1,2,\cdots,n$ 有正整数解. 因此，对每个正整数解 x，都有 $P(x)$ 被 $p_1p_2\cdots p_n$ 整除.

6. 解法1 令 $p_1, p_2, \cdots, p_s$ 是 s 个相异素数，由中国剩余定理，下列同余式组

$x\equiv -1 \pmod{p_1^2}$,

$x\equiv -2 \pmod{p_2^2}$,

……

$x\equiv -s \pmod{p_s^2}$

存在一解，设此解为 n.

则 s 个连续整数 $n+1, n+2, \cdots, n+s$ 每个都有一个二重素因子，即有

$p_i^2 \mid n+i$.

取 $s=1000000$，则可得到满足题目要求的1000000个连续整数.

解法2 我们用数学归纳法证明：

存在 s 个连续的整数，使得每一个都含有二重素因子.

(1) 当 $s=1$ 时，只要取一个素数的平方即可，比如取 $4=2^2$，则 $s=1$ 时命题成立.

(2) 假设当 $s=k$ 时命题成立.

即有 k 个连续整数 $n+1, n+2, \cdots, n+k$，它们分别含有二重的素因子 $p_1^2, p_2^2, \cdots, p_k^2$.

那么，任取一个与 $p_1, p_2, \cdots, p_k$ 都不同的素数 p_{k+1}，当 $t=1, 2, \cdots, p_{k+1}^2$ 时，数

$$tp_1^2p_2^2\cdots p_k^2+n+k+1 \quad ①$$

是 p_{k+1}^2 个不同的数. 这 p_{k+1}^2 个数任两数之差是形如

$ap_1^2p_2^2\cdots p_k^2, 1\leqslant a\leqslant p_{k+1}^2-1$

的数，这些数不能被 p_{k+1}^2 整除.

于是把①中的数除以 p_{k+1}^2 的余数两两不同，但是，除以 p_{k+1}^2 的余数只有

$0, 1, 2, \cdots, p_{k+1}^2-1$

共 p_{k+1}^2 个，所以，一定存在一个数 t_0 $(1\leqslant t_0\leqslant p_{k+1}^2)$，使得

$t_0p_1^2p_2^2\cdots p_k^2+n+k+1$

能被 p_{k+1}^2 整除，于是

$t_0p_1^2p_2^2\cdots p_k^2+n+i, i=1, 2, \cdots, k, k+1$

分别能被 $p_1^2, p_2^2, \cdots, p_k^2, p_{k+1}^2$ 整除.

从而命题对 $s=k+1$ 成立.

由 (1)，(2)，对所有自然数 s，命题成立.

取 $s=1000000$ 即为本题.

7. 首先证明，对每一个正整数 n，它至少适合下列一组同余式中的一个同余式（这样的一组同余式称为覆盖同余式）：

$n\equiv1\pmod 2$， ①

$n\equiv1\pmod 3$， ②

$n\equiv2\pmod 4$， ③

$n\equiv4\pmod 8$， ④

$n\equiv0\pmod{12}$， ⑤

$n\equiv8\pmod{24}$. ⑥

事实上，如果 n 为奇数，那么它适合①；如果 n 为偶数，但不是 4 的倍数，那么它适合③；如果 n 为 4 的倍数，但不是 8 的倍数，那么它适合④；如果 n 为 8 的倍数，设 $n=8m$，那么当 m 是 3 的倍数时，n 适合⑤，当 m 除以 3 余 1 时，n 适合⑥，当 m 除以 3 余 2 时，n 适合②.

于是 n 至少适合同余式①～⑥中的一个同余式.

注意到

$2^2\equiv1\pmod 3$，$2^3\equiv1\pmod 7$，$2^4\equiv1\pmod 5$，

$2^8\equiv1\pmod{17}$，$2^{12}\equiv1\pmod{13}$，$2^{24}\equiv1\pmod{241}$.

当 n 适合同余式①时，即 $n=2m+1$，则

$k\cdot2^n+1=k\cdot2^{2m+1}+1=2k\cdot4^m+1\equiv2k+1\pmod 3$.

同样，当 n 适合②，③，④，⑤，⑥时，分别有

$k\cdot2^n+1\equiv2k+1\pmod 7$，

$k\cdot2^n+1\equiv4k+1\pmod 5$，

$k\cdot2^n+1\equiv16k+1\pmod{17}$，

$k\cdot2^n+1\equiv k+1\pmod{13}$，

$k\cdot2^n+1\equiv256k+1\pmod{241}$.

因此，只要 k 适合下面的同余方程组：

$2k+1\equiv0\pmod 3$，

$2k+1\equiv0\pmod 7$，

$4k+1\equiv0\pmod 5$，

$16k+1\equiv0\pmod{17}$，

$k+1\equiv0\pmod{13}$，

$256k+1\equiv0\pmod{241}$.

则 $k\cdot2^n+1$ 至少被 3，7，5，17，13，241 中的某一个整除，从而 $k\cdot2^n+1$ 为合数.

注意，若 k 满足

$2k+1\equiv0\pmod 3$，

则由 $2k+1=3m$ 知，m 为奇数，设 $m=2t+1$，便有 $2k+1=6t+3$，$k=3t+1$，因而有

$k\equiv1 \pmod 3$.

同理，可把上面的同余方程组化为下面等价的同余方程组

$k\equiv1 \pmod 3$,

$k\equiv3 \pmod 7$,

$k\equiv1 \pmod 5$,

$k\equiv1 \pmod{17}$,

$k\equiv-1 \pmod{13}$,

$k\equiv16 \pmod{241}$.

根据中国剩余定理（即孙子定理），设 m_1，m_2，…，m_n 两两互素，则同余方程组 $x\equiv a_i \pmod{m_i}$，$i=1$，2，…，n 一定有整数解.

由于 3，7，5，17，13，241 都是素数，则上述同余方程组一定有解，因而一定存在整数 k，使 $k\cdot2^n+1$ 对每一个 n 都是合数，且可具体算出 $k=1207426+5592405m$，m 为非负整数.

8. 有一个常识性的结论：素数有无穷多个（这个结论的证明略）. 于是我们可以找到 $2r$ 个不同素数 $p_1<q_1<p_2<q_2<\cdots<p_r<q_r$.

考虑同余方程组 $x\equiv-i \pmod{p_iq_i}$ $(1\leqslant i\leqslant r)$. 由中国剩余定理知它必存在解 x_0. 不妨设 $x_0>0$（否则用 $x_0+p_1q_1p_2q_2\cdots p_rq_r\cdot N$，$N$ 为充分大的正整数来代替 x_0 讨论），则 x_0+i 可以被 p_iq_i 整除$(1\leqslant i\leqslant r)$，所以我们找到了 r 个连续正整数 x_0+1，x_0+2，x_0+3，…，x_0+r，它们均不是素数的幂.

原命题得证.

9.（反证法）假设命题不成立，则存在整数 x_i，使得 $F(x_i)$ 不是 a_i 的倍数，$i=1$，2，…，m.

于是存在整数 $d_i=p_i^{\alpha_i}$，其中 p_i 为素数，α_i 为正整数，使得 a_i 能被 d_i 整除，但 $F(x_i)$ 却不能被 d_i 整除. 在 d_1，d_2，…，d_m 中如果存在有同一个素数的方幂，则仅保留其中幂次最低的，去掉那些幂次较高的，这样便得到一个两两互素的数组，不妨设为 d_1，d_2，…，d_s.

由中国剩余定理知，存在整数 N，使得 $N\equiv x_i \pmod{d_i}$，$i=1$，2，…，s.

又因为 $F(x)$ 是整系数多项式，所以 $F(x)-F(y)$ 能被 $x-y$ 整除，从而 $F(N)$ 不能被 $d_1,d_2,\cdots,d_s$ 整除，由 $d_1,d_2,\cdots,d_s$ 的选取即知不能被 $d_1,d_2,\cdots,d_m$ 整除，因此也就不能被 $a_1,a_2,\cdots,a_m$ 中任何一个数整除，与题设矛盾.

第十四章　二次剩余

1. 首先证明，对任给的 k，存在一个正整数 a_k，满足 $a_k^2\equiv-7 \pmod{2^k}$，关于 k 用数学归纳法进行证明.

直接观察表明，当 $k\leqslant3$ 时，取 $a_k=1$ 便可满足条件，设对某个 $k>3$，我们有 $a_k^2\equiv-7 \pmod{2^k}$.

下面考虑 a_k^2 模 2^{k+1} 的值，它或者为 $a_k^2\equiv-7 \pmod{2^{k+1}}$ 或者为 $a_k^2\equiv2^k-7 \pmod{2^{k+1}}$. 对于前者，可取 $a_{k+1}=a_k$；对于后者，可取 $a_{k+1}=a_k+2^{k-1}$. 这是由于 $k\geqslant3$，及 a_k 为奇数，所以 $a_{k+1}^2=a_k^2+2^ka_k+2^{2k-2}\equiv a_k^2+2^k\equiv-7 \pmod{2^{k+1}}$.

上式的推出利用了归纳假设.

最后，容易看出，序列 $\{a_k\}$ 没有最大元素. 因而可要求对任何正整数 k，$a_k^2 \geqslant 2^k-7$. 因而 $\{a_k\}$ 包含了无穷多个不同的值，因而命题成立.

2. 若方程有正整数解 x，y，方程两边同乘以 4，得 $4(x^2+3xy-2y^2)=488$，即

$(4x^2+12xy+9y^2)-17y^2=17\times29-5$，

所以 $(2x+3y)^2\equiv-5 \pmod{17}$. ①

只需注意 -5 不是模 17 的二次剩余，所以①式无解. 所以原方程无解.

3. 用反证法：方程 $3y^2=(x^2+1)x$ 有一组整数解 x，y. 由 x 与 x^2+1 是互素的，即存在正整数 u，v，使得 $y=u\cdot v$，且 $3u^2=x^2+1$，$v^2=x$ 或 $u^2=x^2+1$，$3v^2=x$.

前一种情况显然不可能，现假定后一种情况成立.

注意到，这时 $u^2=(x+1)(x^2-x+1)$.

由于 $x\equiv0 \pmod 3$，而 $x^2-x+1=(x+1)(x-2)+3$，又 $x+1$ 与 x^2-x+1 是互素的，

因此，存在 t 满足 $x^2-x+1=t^2$，容易看出，方程 $x^2-x+1=t^2$ 只有一个正整数 $x=1$，但这与 $x\equiv0 \pmod 3$ 矛盾.

因此，题目结论成立.

4. 对于 (1)，我们可利用欧拉判别法证明：$x_0=\pm a^{m+1}$ 是 $x^2\equiv a \pmod p$ 的解. 对于 (2)，我们利用欧拉判别法及 $\left(\frac{-2}{p}\right)=-1$. 解的形式可分开来写：

当 $a^{2m+1}\equiv1 \pmod p$ 时，$x_0\equiv\pm a^{m+1}$，

当 $a^{2m+1}\equiv-1 \pmod p$ 时，$x_0\equiv\pm2^{2m+1}a^{m+1}$.

注 $\left(\frac{-2}{p}\right)=(-1)$ 的证明需要用到 Gauss 引理，可查看有关书籍.

5. 假设这样的素数只有有限多个，设它们为 p_1，p_2，…，p_k.

我们考虑 $(2p_1\cdots p_k)^2+1=p$. 由假设及 $p\equiv1 \pmod 4$，所以 p 不是素数，设 p_0 是 p 的素因子，p_0 当然是奇数，所以 -1 是模 p_0 的二次剩余，即 $\left(\frac{-1}{p_0}\right)=1$，从而 $p_0\equiv1 \pmod 4$，但 p_0 显然不是 p_1，p_2，…，p_k，这与假设矛盾.

所以形如 $4k+1$ 的素数有无穷多个.

6. 首先不加证明地指出 $\left(\frac{2}{p}\right)=1\Leftrightarrow p\equiv1 \pmod 8$. 设 p 是 x^4+1 的奇素因数，即 $(x^2)^2\equiv x^4\equiv-1 \pmod p$，由 $\left(\frac{-1}{p}\right)=1$，推出 $p\equiv1 \pmod 4$.

而另一方面 $x^4+1=(x^2+1)^2-2x^2$，所以有 $(x^2+1)^2\equiv2x^2 \pmod p$.

由 $(p,2x)=1$，利用 Legendre 符号的性质

$1=\left(\frac{(x^2+1)^2}{p}\right)=\left(\frac{2x^2}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{x^2}{p}\right)-\left(\frac{2}{p}\right)$.

从而推出 $p\equiv\pm1 \pmod 8$.

而由 $p\ x^4+1$，从而必有 $p\equiv1 \pmod 8$.

下面证明原命题，若这样的素数只有有限个，设为 $p_1,p_2,\cdots,p_k$. 考虑 $p=(2p_1p_2\cdots p_k)^4+1$，由

假设及 $p\equiv1 \pmod 8$ 知 p 不是素数，设 p_0 是 p 的素因子，当然 p_0 是奇数.

由已证结论知 $p_0\equiv1 \pmod 8$，但 p_0 不是 $p_1,p_2,\cdots,p_k$ 中的任一个，矛盾.

所以，有无限多个 $8k+1$ 型的素数.

7. 记 $S=\{a\mid f(a)=f(1),a\in\mathbf{N}^*\}$，由条件(2)可知

$$f(a)+f(a^2+1)=f(a)+f(1),$$

所以 $a^2+1\in S,a\in\mathbf{N}^*$.

设 p 为任意 $4k+1$ 型素数，则

$$\left(1\cdot2\cdot\cdots\cdot\frac{p-1}{2}\right)^2\equiv1\cdot2\cdot\cdots\cdot\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot\cdots\cdot(p-1)\equiv-1 \pmod p,$$

所以 $\left(1\cdot2\cdot\cdots\cdot\frac{p-1}{2}\right)^2+1\equiv0 \pmod p$.

由 (1) 可知 $f(p)\geqslant f\left(\left(1\cdot2\cdot\cdots\cdot\frac{p-1}{2}\right)^2+1\right)=f(1)$，又由(1)知 $f(p)\leqslant f(1)$，所以

$f(p)=f(1),p\in S$.

若 $a,b\in S$，则知 $f(ab)+f(a^2+b^2)=2f(1)\geqslant f(ab)+f(a^2+b^2)$，所以

$ab\in S,a^2+b^2\in S$.

而 $2\in S$，故对任意数 a，a 不含 $4k+3$ 型素因数，则 $a\in S$.

设 $a\in S$，则 $a^2+b^2\in S$. 若不然，则 a^2+b^2 含有一个 $4k+3$ 型素因数，因而

$a^2\equiv-b^2 \pmod p$，可知 $a\not\equiv0 \pmod p$.

所以 $(a^2)^{\frac{p-1}{2}}\equiv a^{p-1}\equiv1\equiv(-b^2)^{\frac{p-1}{2}}\equiv-1 \pmod p$，矛盾！

所以

$$f(ab)+f(a^2+b^2)=f(ab)+f(1)=f(a)+f(b)=f(1)+f(b),$$

所以 $\quad f(ab)=f(b),\forall b\in\mathbf{N}^*,a\in S$ 成立. ①

令 $a=t,b=qt,q,t\in\mathbf{N}^*$，则 $q^2+1\in S$，所以 $f(t^2(q^2+1))=f(t^2)$.

又 $f(t\cdot qt)+f(t^2(q^2+1))=f(t)+f(qt)$，

所以 $\quad f(qt^2)+f(t^2)=f(t)+f(qt)$. ②

因为 $t\mid t^2,qt\mid qt^2$，所以

$f(t)\geqslant f(t^2),f(qt)\geqslant f(qt^2)$，

所以 $f(qt^2)=f(qt),f(t)=f(t^2),\forall q,t\in\mathbf{N}^*$ 成立.

设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\cdots q_t^{\beta_t}$，其中 $\alpha_i,\beta_i\geqslant1$，$p_i$ 为 2 或 $4k+1$ 型素数，q_i 为 $4k+3$ 型素数，则知当 $t=0$ 时，$f(n)=f(1)$，当 $t>0$ 时，

$f(n)=f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\cdots q_t^{\beta_t})\quad f(q_1q_2\cdots q_t)$（此由①，②可得）.

而当 $(p,q)=1$ 时，$p^2+q^2\in S$[否则 $(p,q)>1$]，所以

$f(pq)+f(p^2+q^2)=f(p)+f(q)$，

所以 $\quad f(pq)=f(p)+f(q)-f(1)$，

故 $\quad f(n)=f(q_1q_2\cdots q_t)=f(q_1)+f(q_2)+\cdots+f(q_t)-(t-1)f(1)$.

设 $q_1<q_2<\cdots<q_k<\cdots$ 为所有从小到大排列的 $4k+3$ 型素数，设 $f(1)=a_0$，$f(q_i)=t_i$，

其中 $t_i \leqslant a_0$，t_i，$a_0 \in \mathbf{Z}$，$i=1,2,\cdots$，则依上可知：

当 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}$ 时，其中 p_i 为 2 或 $4k+1$ 型素数，q_i 为 $4k+3$ 型素数，$f(n)=a_0$，当 $s=0$ 时；$f(n)=t_{i_1}+t_{i_2}+\cdots+t_{i_s}-(s-1)a_0$，当 $s>0$ 时.

下面只需验证以上定义的函数满足条件.

由于 $t_i \leqslant a_0$，由以上定义易知：当 $a\mid b$ 时，$f(a)\geqslant f(b)$，故满足 (1).

下证满足 (2).

若 a，b 中有一个属于 S，不妨设 $a\in S$，则易知 $a^2+b^2\in S$，所以

$f(a)=f(a^2+b^2)=a_0$，

所以 $f(ab)+f(a^2+b^2)=f(b)+f(a)$.

若 a，b 均不属于 S，不妨设 $a=p_1q_1t$，$b=p_2q_2t$，其中 p_1，p_2 不含 $4k+3$ 型素因数，q_1t，q_2t 不含 2 及 $4k+1$ 型素因数，$(q_1,q_2)=1$，则由定义

$f(a)=f(q_1t)$，$f(b)=f(q_2t)$，

$f(ab)=f(q_1q_2t)$，$f(a^2+b^2)=f(t)$，

[因为 $(p_1q_1)^2+(p_2q_2)^2\in S$]

所以只需验证 $f(q_1t)+f(q_2t)=f(q_1q_2t)+f(t)$.

由定义不妨设 q_1，q_2，t 均不含有平方因子. 设

$t=rst_0$，$q_1=rm$，$q_2=sn$，

其中 $(m,st_0)=(n,rt_0)=1$，则知

$(r,m)=1,(s,n)=1,(r,s)=1,(r,t_0)=1,(s,t_0)=1$，

所以 $f(q_1t)=f(rsmt_0)$，

$f(q_2t)=f(rsnt_0)$，

$f(q_1q_2t)=f(mnt_0rs)$，

$f(t)=f(rst_0)$，

所以
$$f(q_1t)+f(q_2t)=f(rsmt_0)+f(rsnt_0)=2f(r)+2f(s)+2f(t_0)+f(m)+f(n)-6f(1)$$
$$=f(mnt_0rs)+f(rst_0).$$

由定义知 $f(pq)=f(p)+f(q)-f(1)$，当 $(p,q)=1$ 时. 从而以上定义的函数满足条件.

即当 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\cdots q_t^{\beta_t}$，$p_i$ 为 2 或 $4k+1$ 型素数，q_i 为 $4k+3$ 型素数，α_i，$\beta_i\geqslant 1$，则

$$f(n)=\begin{cases}a_0, & \text{当 } t=0 \text{ 时},\\ t_{i_1}+t_{i_2}+\cdots+t_{i_t}-(t-1)a_0, & \text{当 } t>0 \text{ 时},\end{cases}$$

其中 $f(q_i)=t_i\leqslant a_0=f(1)$，$t_i$，$a_0$ 为任意整数，$t_i\leqslant a_0$.

8. 所求的充要条件是：4 不整除 n 并且对每个模 4 余 3 的素数 q，都有 $q\nmid n$.

必要性：若 n 是 4 的倍数，则若 $n=a^2+b^2 \pmod 4$ 易知只可能是

$a^2\equiv b^2\equiv 0 \pmod 4$，即 $2\mid(a,b)$，矛盾.

若 $q\equiv 3 \pmod 4$ 素数，且 $q\mid n$，则若 $n=a^2+b^2$，必有 $q\mid(a,b)$.

否则设 q 不整除 a. 由 $q\mid n$ 知 q 不整除 b，所以

$$1=\left(\frac{a^2}{q}\right)=\left(\frac{n-b^2}{q}\right)=\left(-\frac{b^2}{q}\right)=\left(\frac{-1}{q}\right)=-1$$

(Legrendre 符号),矛盾.

充分性:先设 n 为奇数. 只考虑 $n>1$. 令 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$($p_1<p_2<\cdots<p_k$ 都为模 4 余 1 的素数,$\alpha_j\in\mathbf{N}^*$). 熟知存在 $a_j,b_j\in\mathbf{N}^*$ 使

$$p_j=a_j^2+b_j^2=(a_j+b_j\mathrm{i})(a_j-b_j\mathrm{i}),$$

于是

$$n=\prod_{j=1}^{k}(a_j+b_j\mathrm{i})^{\alpha_j}\prod_{j=1}^{k}(a_j-b_j\mathrm{i})^{\alpha_j}\ (\mathrm{i}\ 为虚数单位).$$

现在令 $x,y\in\mathbf{Z}$ 使 $x+y\mathrm{i}=\prod\limits_{j=1}^{k}(a_j+b_j\mathrm{i})^{\alpha_j}$,则

$$x-y\mathrm{i}=\prod_{j=1}^{k}(a_j-b_j\mathrm{i})^{\alpha_j},$$

所以 $\quad n=(x+y\mathrm{i})(x-y\mathrm{i})=x^2+y^2$.

下面证明:x 和 y 互素.

若否,设存在素数 $p\mid(x,y)$,则 $p\mid n$,即 $p=p_l$ 对某个 $1\leqslant l\leqslant k$ 成立. 因此在 $\mathbf{Z}[\mathrm{i}]$ 中,$p_l\mid x\pm y\mathrm{i}$,从而可知 $a_l+b_l\mathrm{i}\mid\prod\limits_{j=1}^{k}(a_j-b_j\mathrm{i})^{\alpha_j}$,从而 $a_l+b_l\mathrm{i}$ 为 $\mathbf{Z}[\mathrm{i}]$ 中的素数,故 $a_l+b_l\mathrm{i}\mid a_t-b_t\mathrm{i}$ 对某个 t 成立. 但在 $\mathbf{Z}[\mathrm{i}]$ 中两个不同素数不互相整除,矛盾. 所以 x 和 y 互素.

在 n 为偶数时,$\frac{n}{2}$ 是奇数(否则 $4\mid n$). 令 $\frac{n}{2}=a^2+b^2(2\nmid a+b,(a,b)=1)$,则

$n=(a+b)^2+(a-b)^2$ 且 $(a+b,a-b)=1$.

充分性获证.

9. 先证必要性. 设有整数 a,使得 $a^2\equiv-1(\bmod p)$,显然 $p\nmid a$,故由费马小定理知

$1\equiv a^{p-1}\equiv(a^2)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}(\bmod p)$,从而 $\frac{p-1}{2}$ 应为偶数,即 $p\equiv1(\bmod 4)$.

再证充分性. 若 $p\equiv1(\bmod 4)$,即 $\frac{p-1}{2}$ 为偶数,于是

$$\begin{aligned}(p-1)!&=1\times2\times\cdots\times\frac{p-1}{2}\times(p-1)\times(p-2)\times\cdots\times\left(p-\frac{p-1}{2}\right)\\&\equiv1\times2\times\cdots\times\frac{p-1}{2}\times(-1)\times(-2)\times\cdots\times\left(-\frac{p-1}{2}\right)\times(\bmod p)\\&=(-1)^{\frac{p-1}{2}}\times1^2\times2^2\times\cdots\times\left(\frac{p-1}{2}\right)^2\\&=\left[\left(\frac{p-1}{2}\right)!\right]^2.\end{aligned}$$

从而由威尔逊定理即知 $\left[\left(\frac{p-1}{2}\right)!\right]^2\equiv-1(\bmod p)$.

注 本例的这个结论十分重要,我们利用它便可以证明形如 $4n+1,n=1,2,\cdots$ 的素数有无限多个.

(反证法)假设形如 $4n+1$ 的素数只有有限个,记为 $p_1,p_2,\cdots,p_k$,我们考虑数 $4(p_1p_2\cdots p_k)^2+1$,设它的一个奇素因子为 p,则 -1 是模 p 的平方剩余,从而 p 为形如 $4n+1$ 的素数,但易见 p 不同

于 $p_1, p_2, \cdots, p_k$，矛盾.

10. 设 $f(x)=(x-1)(x-2)\cdot\cdots\cdot[x-(p-1)]=x^{p-1}+\sum\limits_{l=1}^{p-1}(-1)^l A_l x^{p-1-l}$，

$g(x)=x^{p-1}-1$，

则同余方程 $f(x)\equiv 0(\bmod p)$ 有 $p-1$ 个解 $x=1,2,\cdots,p-1$.

由费马小定理可知 $g(x)=0(\bmod p)$ 也有 $p-1$ 个解 $x=1,2,\cdots,p-1$，从而同余方程 $f(x)-g(x)\equiv 0(\bmod p)$ 至少有 $p-1$ 个解. 但是

$$f(x)-g(x)=\sum_{l=1}^{p-2}(-1)^l A_l x^{p-1-l}+(p-1)!+1$$

是 $p-2$ 次多项式，故由拉格朗日定理知 $f(x)-g(x)$ 的各项系数均能被 p 整除，即有 $(p-1)!\equiv -1(\bmod p)$.（这里实际上给出了威尔逊定理的另一种证明）

$A_l\equiv 0(\bmod p)$，于是(1)得证.

$$f(x)=(x-1)(x-2)\cdot\cdots\cdot[x-(p-1)]=(-x+1)(-x+2)\cdot\cdots\cdot(-x+p-1)$$
$$=[(-x+p)-1][(-x+p)-2]\cdot\cdots\cdot[(-x+p)-(p-1)]=f(p-x),$$

即 $f(x)=f(p-x)$. 将 x 换成 $-x$ 即得 $f(-x)=f(p+x)$，从而

$$x^{p-1}+\sum_{l=1}^{p-2}A_l x^{p-1-l}+(p-1)!=(x+p)^{p-1}+\sum_{l=1}^{p-2}(-1)^l A_l(x+p)^{p-1-l}+(p-1)!. \qquad ①$$

对①模 p^2 并利用(1)可得

$$x^{p-1}+\sum_{l=1}^{p-2}A_l x^{p-1-l}\equiv x^{p-1}+(p-1)px^{p-2}+\sum_{l=1}^{p-2}(-1)^l A_l x^{p-1-l}(\bmod p^2)$$，即

$$\sum_{l=1}^{p-2}[1+(-1)^{l+1}]A_l x^{p-1-l}\equiv p(p-1)x^{p-2}(\bmod p^2).$$

从而当 l 为奇数且 $1<l<p$ 时，有 $A_l\equiv 0(\bmod p^2)$.

11. 记 $f(x)=(xp-1)(xp-2)\cdots(xp-p+1)(x\in\mathbf{Z}^+)$，则 C_{ap}^{bp} 可以写成

$$\frac{(ap)(ap-p)\cdots(ap-bp+p)}{(bp)(bp-p)\cdots(p)}\cdot\frac{f(a)f(a-1)\cdots f(a-b+1)}{f(b)f(b-1)\cdots f(1)}$$
$$=C_a^b\cdot\frac{f(a)f(a-1)\cdots f(a-b+1)}{f(b)f(b-1)\cdots f(1)}.$$

故 $C_{ap}^{bp}=\dfrac{C_a^b}{f(b)f(b-1)\cdots f(1)}[f(a)f(a-1)\cdots f(a-b+1)-f(b)f(b-1)\cdots f(1)]$.

再注意到 $p\nmid f(b)f(b-1)\cdots f(1)$，故欲证 $C_{ap}^{bp}\equiv C_a^b(\bmod p^3)$，只要证

$$f(a)f(a-1)\cdots f(a-b+1)\equiv f(b)f(b-1)\cdots f(1)(\bmod p^3). \qquad ①$$

可隐约猜到能证明如下之引理：$f(x)\equiv(p-1)!\ (\bmod p^3)$，$\forall x\in\mathbf{Z}$.

事实上，如果记 $\sigma_0=1$，以及 $k\geqslant 1$ 时，$\sigma_k=\sum\limits_{1\leqslant i_1<i_2<\cdots<i_k\leqslant p-1} i_1\cdot i_2\cdot\cdots\cdot i_k$，则由韦达定理，

$$f(xp)=\sum_{k=0}^{p-1}(xp)^k\cdot(-1)^{p-1-k}\sigma_{p-1-k}\equiv\sigma_{p-1}-xp\sigma_{p-2}+x^2p^2\sigma_{p-3}(\bmod p^3). \qquad ②$$

如果我们能证明 $p\mid\sigma_{p-3}$， ③

$p^2\ \sigma_{p-2}$， ④

则引理显然成立(根据②).③④是经典的结论,为了方便地证明③,④,我们采取一种简便的表示方法:

如果 $s\equiv tr \pmod m$,且 m 与 t 互素,则简记 $\frac{s}{t}\equiv r \pmod m$.

设 $\frac{s_1}{t_1}\equiv r_1 \pmod m$,$\frac{s_2}{t_2}\equiv r_2 \pmod m$,不难证明 $\frac{s_1}{t_1}+\frac{s_2}{t_2}\equiv r_1+r_2 \pmod m$.

且若 $s_1\equiv s_2 \pmod m$,$t_1\equiv t_2 \pmod m$,则 $r_1\equiv r_2 \pmod m$.

在这种记号下来证明③④:

$$\begin{aligned}\sigma_{p-3}&\equiv(p-1)!\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij}\equiv(p-1)!\sum_{1\leqslant i<j\leqslant p-1}i^{-1}j^{-1} \pmod p\\&\equiv\frac{(p-1)!}{2}\sum_{i\neq j}i^{-1}j^{-1} \pmod p\equiv\frac{(p-1)!}{2}\sum_{\substack{s\neq t\\1\leqslant s,t\leqslant p-1}}st \pmod p\\&\equiv\frac{(p-1)!}{2}\cdot\left\{\left[\frac{p(p-1)}{2}\right]^2-\frac{(p-1)p(2p-1)}{6}\right\}\\&\equiv 0 \pmod p,\text{③ 得证.}\end{aligned}$$

$$\sigma_{p-2}=(p-1)!\sum_{i=1}^{p-1}\frac{1}{i}=p!\sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)},\qquad ⑤$$

而 $\displaystyle\sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)}\equiv\sum_{i=1}^{\frac{p-1}{2}}-(i^{-1})^2 \pmod p$.

容易证明,对每个 $1\leqslant i\leqslant\frac{p-1}{2}$,存在唯一的 $1\leqslant j\leqslant\frac{p-1}{2}$,使 $(i^{-1})^2\equiv j^2 \pmod p$.

(事实上,设 $i^{-1}\in\{1,2,\cdots,p-1\}$,若 $2i^{-1}>p-1$,取 $j=p-i^{-1}$,若 $2i^{-1}\leqslant p-1$,则取 $j=i^{-1}$.而 j 的唯一性则显然.)

所以 $\displaystyle\sum_{i=1}^{\frac{p-1}{2}}\frac{1}{i(p-i)}\equiv\sum_{j=1}^{\frac{p-1}{2}}(-j^2) \pmod p\equiv-\frac{p(p^2-1)}{24}\equiv 0 \pmod p$,

代入⑤得 $p^2\mid\sigma_{p-2}$,④得证.

由引理马上得知①左边和右边模 p^3 均同余于 $[(p-1)!]^p$,故①成立.

从而原命题得证.

注 若利用费马定理、威尔逊定理及拉格朗日定理,③④有如下的简证.为此,我们设 $g(t)=(t+1)(t+2)\cdots(t+p-1)=t^{p-1}+\sigma_1\cdot t^{p-2}+\cdots+\sigma_{p-3}t^2+\sigma_{p-2}t+(p-1)!$,则当 $t=1,2,\cdots,p-1$ 时,均有 $f(x)\equiv 0 \pmod p$,而由费马小定理可知,当 $1\leqslant t\leqslant p-1$ 时,$t^{p-1}\equiv 1 \pmod p$,由威尔逊定理知 $(p-1)!\equiv 0 \pmod p$,所以 $p-2$ 次同余方程 $g(t)-[t^{p-1}+(p-1)!]\equiv 0 \pmod p$ 有 $p-1$ 个不同解($\bmod\ p$ 意义下),故由拉格朗日定理知:$\sigma_1,\cdots,\sigma_{p-3},\sigma_{p-2}$ 都是 p 的倍数,即 $p\mid\sigma_{p-3}$,$p\mid\sigma_{p-2}$.

再注意到在 $g(t)$ 中令 $t=-p$,结合 p 为奇素数,有

$$\begin{aligned}g(-p)&=(-1)^{p-1}\cdot(p-1)!\\&=(-p)^{p-1}+\cdots+\sigma_{(p-3)}(-p)^2+\sigma_{p-2}\cdot(-p)+(p-1)!\\&\Rightarrow\sigma_{p-2}+\sigma_{p-3}\cdot(-p)+\cdots+(-p)^{p-2}=0\ (p\geqslant 5).\end{aligned}$$

从而 $p^2 | \sigma_{p-2}$.

第十五章 高斯函数 $[x]$

1. 设 $10^{31}=t$，则

$$\left[\frac{10^{93}}{10^{31}+3}\right]-\left[\frac{t^3}{t+3}\right]=\left[\frac{t^3+3^3}{t+3}-\frac{3^3}{t+3}\right]=t^2-3t+3^2+\left[-\frac{3^3}{t+3}\right]=t^2-3t+3^2-1$$
$$=t(t-3)+8=10^{31}(10^{31}-3)+8.$$

所以 $\left[\frac{10^{93}}{10^{31}+3}\right]$ 的末两位是 08.

2. 因为 503 是素数，所以当 $n=0,1,2,\cdots,502$ 时，$\frac{305n}{503}$ 不是整数.

由于 $\frac{305n}{503}+\frac{305(503-n)}{503}=305$，所以

$\frac{305n}{503}$ 与 $\frac{305(503-n)}{503}$ 的小数部分之和为 1，于是

$$\left[\frac{305n}{503}\right]+\left[\frac{305(503-n)}{503}\right]=304.$$

$$\sum_{n=0}^{502}\left[\frac{305n}{503}\right]=\sum_{n=1}^{502}\left[\frac{305n}{503}\right]=\sum_{n=1}^{251}\left(\left[\frac{305n}{503}\right]+\left[\frac{305(503-n)}{503}\right]\right)=304\cdot 251=76304.$$

3. 当 $k>1$ 时，$\sqrt{k}<k$，则

$$0<\frac{\sqrt{k}}{k}<1,$$

$$\left[\frac{\sqrt{k}}{k}\right]=0.$$

于是 $\left[\frac{k+\sqrt{k}}{k}\right]=\left[1+\frac{\sqrt{k}}{k}\right]=1,(k>1)$.

从而原式 $=1989$.

4. 当 x 为平方数时，

$[\sqrt{x}]+[-\sqrt{x}]=0$；

当 x 为非平方数时，

$[\sqrt{x}]+[-\sqrt{x}]=-1$.

已知的式子中有 $1989\cdot 1990$ 对数，其中有 1989 对平方数，有 1989^2 对非平方数，所以其和为 $-1989^2=-3956121$.

5. 由公式 $\left(\frac{a+b}{2}\right)^2\leqslant\frac{a^2+b^2}{2}$ 可得

$$\left(\frac{\sqrt{n}+\sqrt{n+1}}{2}\right)^2\leqslant\frac{n+n+1}{2}=\frac{4n+2}{4}.$$

从而 $\sqrt{n}+\sqrt{n+1}\leqslant\sqrt{4n+2}$.

再由函数 $[x]$ 的单调性，$[\sqrt{n}+\sqrt{n+1}]\leqslant[\sqrt{4n+2}]$.

假设对某个正整数 n,有 $[\sqrt{n}]+[\sqrt{n+1}]\neq[\sqrt{4n+2}]$,则

$[\sqrt{n}+\sqrt{n+1}]<[\sqrt{4n+2}]$.

令 $p=[\sqrt{4n+2}]$,则

$\sqrt{n}+\sqrt{n+1}<p\leqslant\sqrt{4n+2}$.

平方后得 $2n+1+2\sqrt{n(n+1)}<p^2\leqslant 4n+2$,即

$2\sqrt{n(n+1)}<p^2-2n-1\leqslant 2n+1$,即

$4n(n+1)<(p^2-2n-1)^2\leqslant 4n^2+4n+1$.

由于 $4n^2+4n$ 与 $4n^2+4n+1$ 是两个相继整数,而 $(p^2-2n-1)^2$ 也是整数,于是

$(p^2-2n-1)^2=4n^2+4n+1$,

$p^2=4n+2$.

然而任何整数的平方不能被 4 除余 2,于是出现矛盾.

因此,对每一个正整数 n,都有

$[\sqrt{n}]+[\sqrt{n+1}]=[\sqrt{4n+2}]$.

6. 注意到,

若 $x\in M=\{n^2,n^2+1,\cdots,(n+1)^2-1\}$,则

$[\sqrt{x}]=n$.

而 M 中有 $2n+1$ 个元素,从而

$[\sqrt{n^2}]+[\sqrt{n^2+1}]+\cdots+[\sqrt{(n+1)^2-1}]=n\cdot(2n+1)$.

由于 $44^2=1936$,所以

$[\sqrt{1}]+[\sqrt{2}]+\cdots+[\sqrt{1935}]=1\cdot 3+2\cdot 5+\cdots+43\cdot 87$.

又 $1988-1936+1=53$,所以

$[\sqrt{1936}]+[\sqrt{1937}]+\cdots+[\sqrt{1988}]=44\cdot 53$.

则有

$S=1\cdot 3+2\cdot 5+\cdots+43\cdot 87+44\cdot 53=58146$.

所以 $[\sqrt{S}]=241$.

7. 设 $m=[\frac{n^2}{5}]$.

(1) $n=5k$ (k 是自然数) 时,

$m=[\frac{25k^2}{5}]=5k^2$.

当 $k=1$ 时,m 为素数,此时 $n=5$.

(2) $n=5k+1$(k 是非负整数)时,

$m=\left[\frac{(5k+1)^2}{5}\right]=5k^2+2k+[\frac{1}{5}]=k(5k+2)$.

当 $k=1$ 时,m 为素数,此时 $n=6$.

(3) $n=5k+2$(k 是非负整数)时,

$m=\left[\frac{(5k+2)^2}{5}\right]=5k^2+4k=k(5k+4)$.

当 $k=1$ 时，$m=9$ 是合数，因此对所有正整数 k，m 都是合数.

(4) $n=5k+3$（k 是非负整数）时，

$m=\left[\frac{(5k+3)^2}{5}\right]=(5k+1)(k+1)$.

当 $k=0$ 时，$m=1$，当 k 是正整数时，m 是合数.

(5) $n=5k+4$（k 是非负整数）时，

$m=\left[\frac{(5k+4)^2}{5}\right]=(5k+3)(k+1)$.

当 $k=0$ 时，$m=3$ 是素数，当 k 是正整数时，m 是合数. 此时 $n=4$.

所以 $n=4,5,6$ 时，$\left[\frac{n^2}{5}\right]$是素数.

这样的 n 的倒数之和为

$\frac{1}{4}+\frac{1}{5}+\frac{1}{6}=\frac{37}{60}$.

8. 设 $y=x-1$，则

$[y^2]=[x^2-2x+1]=[x^2-2x]+1$，

$[y]^2=([x]-1)^2=[x]^2-2[x]+1$，

于是 $[y^2]=[y]^2$.

(1) 当 $y\geqslant 0$ 时，则

$y^2\geqslant [y]^2>y^2-1$，

所以 $[y]\leqslant y<\sqrt{1+[y]^2}$，

即 $x\in[n+1,1+\sqrt{1+n^2})$，$n=0,1,2,\cdots$.

(2) 当 $y<0$ 时，则

$[y]^2\geqslant y^2\geqslant [y^2]$，

所以必须 y 为整数时，才能有

$[y]^2=[y^2]$.

即 $x=0,-1,-2,\cdots$.

9. 因 $x=[x]+\{x\}$，则已知方程可化为

$[x]\{x\}+[x]-\{x\}=10$，

$([x]-1)(\{x\}+1)=9$.

因为$[x]-1$ 是整数，则$\{x\}+1$ 是有理数.

因为 $0\leqslant\{x\}<1$，故可令$\{x\}=\frac{n}{k}$，其中 $0\leqslant n<k$.

于是有

$([x]-1)(n+k)=9k$.

当 $n=0$ 时，$\{x\}=0$，由已知方程得

$x=10$.
当 $n>0$ 时,可设 $(n,k)=1$,这时
$(n+k,k)=1$.
于是 9 应是 $n+k$ 的倍数,故
$n+k=3$ 或 9.
(1) $n+k=3$ 时,由 $0\leqslant n<k$ 得
$n=1$,$k=2$,
$\{x\}=\frac{1}{2}$,$[x]=7$.
(2) $n+k=9$ 时,
若 $n=1,k=8$,则
$\{x\}=\frac{1}{8}$,$[x]=9$.
若 $n=2,k=7$,则
$\{x\}=\frac{2}{7}$,$[x]=8$.
若 $n=4,k=5$,则
$\{x\}=\frac{4}{5}$,$[x]=6$.
于是已知方程有 5 个解:
$x=10,7\frac{1}{2},9\frac{1}{8},8\frac{2}{7},6\frac{4}{5}$.
10. 由 $\{x\}$ 的定义
$\{\log_2 1\}=0$,
$\{\log_2 2\}=1$,
$\{\log_2 3\}=\{\log_2 4\}=2$,
$\{\log_2 5\}=\{\log_2 6\}=\{\log_2 7\}=\{\log_2 8\}=3$,
……
$\{\log_2 513\}=\{\log_2 514\}=\cdots=\{\log_2 1024\}=10$,
$\{\log_2 1025\}=\cdots=\{\log_2 1991\}=11$.
则所求的和为
$0+1+2^1\cdot 2+2^2\cdot 3+2^3\cdot 4+\cdots+2^9\cdot 10+967\cdot 11=19854$.
11. 设 $x_k=\left[\frac{k^2}{1980}\right]$,则数列 $\{x_k\}$ 是不减数列.
(1) 当 $k\leqslant 44$ 时,由 $44^2=1936<1980$ 可得
$0<\frac{k^2}{1980}<1$.
于是 $x_1=x_2=\cdots=x_{44}=0$.
(2)由于 $k=62$ 时,$62^2=3844<2\cdot 1980$,而 $63^2>2\cdot 1980$,所以

当 $45\leqslant k\leqslant 62$ 时，

$1<\frac{k^2}{1980}<2$.

于是 $x_{45}=x_{46}=\cdots=x_{62}=1$.

由以上可知，数列$\{x_k\}$的前 62 项只有两个不同的数 0 和 1.

下面考察 $k\geqslant 63$ 时的情形.

(3) $y_k=\frac{(k+1)^2}{1980}-\frac{k^2}{1980}=\frac{2k+1}{1980}$.

当 $y_k>1$ 时，x_{k+1} 与 x_k 显然不同.

此时由 $2k+1>1980$ 解得 $k>989$.

于是当 $989<k\leqslant 1980$ 时，所有的 x_k 都不同，即 $x_{990},x_{991},\cdots,x_{1980}$ 这 991 个数是不同的.

(4) 当 $k=989$ 时，

$\left[\frac{989^2}{1980}\right]=494$.

当 $k\leqslant 989$ 时，$y_k<1$，此时 x_k 与 x_{k+1} 或者相同，或者差 1，于是在 $x_1,x_2,\cdots,x_{989}$ 中，必然会出现 $0,1,2,\cdots,494$ 这些不同的整数.

因此，已知数列$\{x_k\}$中，出现不同的数的总数为

$991+495=1486$(个).

12. 设 $n=kp+r(0\leqslant r<p,k\in\mathbf{N}^+)$，则

$$C_n^p=\frac{n(n-1)\cdots(n-p+1)}{p!}$$

$$=\frac{(kp+r)(kp+r-1)\cdots(kp+1)kp(kp-1)\cdots(kp+r-p+1)}{p(p-1)!}$$

$$=\frac{(kp+r)(kp+r-1)\cdots(kp+1)(kp-p+r+1)\cdots(kp-p+p-1)k}{(p-1)!}$$

$$=\frac{(lp+(p-1)!)k}{(p-1)!}(\text{其中 } l\in\mathbf{N}^+)$$

$$=\frac{lk}{(p-1)!}p+k$$

$$\equiv k(\bmod p)[\text{因为}(p,(p-1)!)=1].$$

所以 $C_n^p\equiv k=\left[\frac{n}{p}\right](\bmod p)$.

13. 设 $g(n)=nf(n)(n\geqslant 1)$，则 $g(0)=0$.

对 $k=1,2,\cdots,n$，若 k 不是 n 的因数，则

$\left[\frac{n}{k}\right]-\left[\frac{n-1}{k}\right]=0$;

若 k 是 n 的因数，则

$\left[\frac{n}{k}\right]-\left[\frac{n-1}{k}\right]=1$.

对于 $n\geqslant 1$，设 $d(n)$ 是 n 的正因数的个数，则

$$g(n)=\left[\frac{n}{1}\right]+\left[\frac{n}{2}\right]+\cdots+\left[\frac{n}{n-1}\right]+\left[\frac{n}{n}\right]$$
$$=\left[\frac{n-1}{1}\right]+\left[\frac{n-1}{2}\right]+\cdots+\left[\frac{n-1}{n-1}\right]+\left[\frac{n-1}{n}\right]+d(n)$$
$$=g(n-1)+d(n).$$

故 $g(n)=g(n-1)+d(n)=g(n-2)+d(n-1)+d(n)=\cdots=d(1)+d(2)+\cdots+d(n)$.

从而，$f(n)=\dfrac{d(1)+d(2)+\cdots+d(n)}{n}$.

因此，只要证均有无穷多个 n，使得

$d(n+1)>f(n)$，$d(n+1)<f(n)$.

当 $n=1$ 时，$d(n)=1$.

当 $n\geqslant2$ 时，$d(n)\geqslant2$，等号当且仅当 n 是素数时成立.

因为 $f(6)=\dfrac{7}{3}>2$，所以，由数学归纳法易知，对所有的 $n\geqslant6$，有 $f(n)>2$.

又因为有无穷多个 $n(n\geqslant6)$，使得 $n+1$ 是素数，从而，$d(n+1)=2<f(n)$，这就证明了(2).

又对于所有的正整数 k，$d(2^k)=k+1$，则 $d(1)$，$d(2)$，$\cdots$无界，于是，存在无穷多个 n，使得

$d(n+1)>\max\{d(1),d(2),\cdots,d(n)\}$.

从而，$d(n+1)>f(n)$. 这就证明了(1).

14．**解法 1**　记 $f(x)=[x]+[2x]+[4x]+[8x]+[16x]+[32x]$.

假设方程有一实数解 x，则

$f(x)=12345$.

因为 $f(195)=12285<12345$，$f(196)=12348>12345$，则

$f(195)<f(x)<f(196)$.

又因为 $f(x)$ 是一个不减函数，则

$195<x<196$.

记 $y=x-195$，则 $0<y<1$.

$$f(y)=[x-195]+[2x-2\cdot195]+\cdots+[32x-32\cdot195]$$
$$=f(x)-f(195)=12345-12285$$
$$=60.\qquad ①$$

由于 $0<y<1$，则对一切正整数 n，$0<ny<n$，从而

$[ny]\leqslant n-1$.

因而又有

$$f(y)=[y]+[2y]+[4y]+[8y]+[16y]+[32y]$$
$$\leqslant0+1+3+7+15+31$$
$$=57.\qquad ②$$

①与②矛盾.

因此原方程没有实数解.

解法 2　设 $f(x)=[x]+[2x]+[4x]+[8x]+[16x]+[32x]=12345$. 由性质(6)及性质(3)，得

$f(x)\leqslant[x(1+2+4+8+16+32)]=[63x]\leqslant 63x.$

因为 $f(x)=12345$，所以

$x\geqslant\frac{12345}{63}\approx 195.952.$

又因为 $f(196)=63\times196=12348$，且由性质(4)，知 $f(x)$ 是不减函数，所以方程的解只能在 $(195,196)$ 之内. 设 $x=195+y,y=x-[x]$，$y\in(0,1)$，则

$f(x)=f(195+y)=195\times63+f(y)=12285+f(y)=12285+f(y).$

另一方面

$f(y)=[y]+[2y]+[4y]+[8y]+[16y]+[32y]<0+1+3+7+15+31=57,$

从而 $f(x)=12285+f(y)<12285+57=12342<12345.$

这与已知方程矛盾，故方程没有实数解.

15. 由题设可知，x 必为整数，且 $x\geqslant0$.

令 $\{a\}=a-[a]$，则

$ax=[a]x+\{a\}x,$

从而原方程化为

$x=[ax]=[a]x+[\{a\}x].$ ①

因为 $[a]\geqslant1$，所以①式成立的充要条件是

$[a]=1$，且 $\{a\}x<1.$ ②

因为 $x=0$ 显然是方程的一个解，所以 $[ax]=x$ 只对 $n-1$ 个正整数成立.

又若 $\{a\}x<1,x'<x$，则显然

$\{a\}x'<1.$

故 $\{a\}x<1$ 的正整数解必是 $x=1,2,\cdots,n-1.$

这时有 $\{a\}<\frac{1}{n-1}.$

又当 $x\geqslant n$ 时，x 不是①的解（否则至少有 $n+1$ 个解），即要求 $\{a\}x\geqslant1$ 成立.

由 $\{a\}x\geqslant1$ 及 $x\geqslant n$，因而有 $\{a\}n\geqslant1$，即

$\{a\}\geqslant\frac{1}{n}.$

于是 $\frac{1}{n}\leqslant\{a\}<\frac{1}{n-1}.$

又由 $[a]=1$，则

$1+\frac{1}{n}\leqslant a<1+\frac{1}{n-1}.$

16. 不妨设 $x\geqslant y$，则 $x^2\geqslant1$，$x\geqslant1$. 有下面两种情形：

(1) 当 $x=1$ 时，$y=1$，此时 $f(x,y)=\frac{1}{2}$.

(2) 当 $x>1$ 时，设 $[x]=n$，由定义及性质 (12) 可设 $\{x\}=x-[x]=\alpha$，则 $x=n+\alpha(0\leqslant\alpha<1)$. 于是 $y=\frac{1}{n+\alpha}<1$，因此

$[y]=0, f(x,y)=\dfrac{n+\alpha+\dfrac{1}{n+\alpha}}{n+1}$.

由函数 $g(x)=x+\dfrac{1}{x}$ 在 $x\geqslant 1$ 时是递增的及 $0\leqslant\alpha<1$，可得 $n+\dfrac{1}{n}\leqslant n+\alpha+\dfrac{1}{n+\alpha}<n+1+\dfrac{1}{n+1}$，因此

$$\frac{n+\frac{1}{n}}{n+1}\leqslant f(x,y)<\frac{n+1+\frac{1}{n+1}}{n+1}.$$

设 $a_n=\dfrac{n+\frac{1}{n}}{n+1}=\dfrac{n^2+1}{n^2+n}=1-\dfrac{n-1}{n^2+n}$,

$b_n=\dfrac{n+1+\frac{1}{n+1}}{n+1}=1+\dfrac{1}{(n+1)^2}$,

则 $a_{n+1}-a_n=\dfrac{n-2}{n(n+1)(n+2)}$,

从而 $a_1>a_2=a_3$，$a_3<a_4<\cdots<a_n<\cdots$，$b_1>b_2>\cdots>b_n>\cdots$. 于是当 $x>1$ 时，$f(x,y)$ 的值域为 $[a_2,b_1)$ 即 $\left[\dfrac{5}{6},\dfrac{5}{4}\right)$.

综上所述，$f(x,y)$ 的值域为 $\left\{\dfrac{1}{2}\right\}\cup\left[\dfrac{5}{6},\dfrac{5}{4}\right)$.

第十六章　整数的 p 进位制及应用

习题 A

1. 由于 $100\leqslant\overline{abc}\leqslant 999$，则 $100\leqslant(a+b+c)^3\leqslant 999$. 从而 $5\leqslant a+b+c\leqslant 9$. 当 $a+b+c=5$ 时，$5^3=125\neq(1+2+5)^3$；当 $a+b+c=6$ 时，$6^3=216\neq(2+1+6)^3$；当 $a+b+c=7$ 时，$7^3=343\neq(3+4+3)^3$；当 $a+b+c=8$ 时，$8^3=512=(5+1+2)^3$；当 $a+b+c=9$ 时，$9^3=729\neq(7+2+9)^3$. 于是所求的三位数只有 512.

2. 本题等价于求最小的正整数 b，使得方程 $7b^2+7b+7=x^4$，① 对 x 有整数解. 因为 7 是素数，所以由①式，7 是 x 的约数，为此设 $x=7k$，则①式化为 $b^2+b+1=7^3k^4$. 最小的 b 出现在 k 最小的时候. 取 $k=1$，此时有 $b^2+b+1=343$，$b^2+b-342=0$，即 $(b-18)(b+19)=0$，解得正整数 $b=18$. 即有 $(777)_{18}=(7^4)_{10}$.

3. 将 n 表示成二进制数：$n=(a_ka_{k-1}\cdots a_2a_1)_2$，其中 $a_i=0$ 或 $1, i=1,2,\cdots,k$，于是 $\left[\dfrac{n}{2}\right]=(a_ka_{k-1}\cdots a_2)_2$，$f(n)=f((a_ka_{k-1}\cdots a_1)_2)=f\left(\left[\dfrac{n}{2}\right]\right)+n-2\left[\dfrac{n}{2}\right]=f((a_ka_{k-1}\cdots a_2)_2)+a_1=f((a_ka_{k-1}\cdots a_3)_2)+a_2+a_1=\cdots=a_k+a_{k-1}+\cdots+a_2+a_1$，于是 $f(n)$ 等于 n 的二进制表示中数码 1 的

个数.由于$0<2^{10}-1<1991<2^{11}-1$,故n最多是有11位的二进制数,但n的数码可有10个,但不能有11个1.因此,$f(n)$的最大值为10.

4. (1) 设进位制的基数为b,由题设知,$b>6$,此时可得方程$b^4+6b^3+3b^2+2b+4=(b^2+2b+5)^2$,整理得$2b^3-11b^2-18b-21=0$,即$(b-7)(2b^2+3b+3)=0$.此方程有唯一实根$b=7$,故在7进位制中,16324是125的平方.

(2) 设进位制的基数为b. 由题设知,$b>4$. 此时可得方程$4(1\cdot b+3)=1\cdot b^2+0\cdot b+0$,且$b>4$,从而$b^2-4b-12=0$,求得正数$b=6$,于是题设等式是在6进位制中.

5. 由题设有$\begin{cases}x\cdot b^2+y\cdot b+z=1993, & ①\\ x+y+z=22. & ②\end{cases}$

①−②得$(b-1)[(b+1)x+y]=1971$,所以$(b-1)$是$1971=3^3\cdot73$的约数.

又$b^3>1993$,$b^2<1993$,所以$12<b<45$,从而$b-1=3^3=27$,即$b=28$.

又$1993=2\cdot28^2+15\cdot28+5$,故$x=2$,$y=15$,$z=5$,$b=28$.

6. (1) 注意到$7=(111)_2$,$2^n-1=(\underbrace{11\cdots11}_{n位})_2$,显然,当且仅当后者位长是前者位长的整数倍或被除数为零时才有所要求的结论,即应有$n=3k$(k为非负整数)为所求.

(2) 注意到$2^n+1=(1\underbrace{00\cdots0}1)_2$,观察除法竖式(略),施行每步除法所得余数皆为1,再注意到末位的组成. 故施行最后一步除法时被除单元只可能是三种情况:$(1001)_2$,$(101)_2$,$(11)_2$,皆不能被$(111)_2$整除,故得证.

7. 因对任一实数,在不同的数制下,整数部分仍是整数部分,小数部分仍是小数部分,而分析被加式的结构应归于二进制解较易.

令$n=(a_ma_{m-1}\cdots a_1a_0)_2$,其中$a_m=1$,$a_i=0$或$1$,$i=0,1,\cdots,m-1$,则$\left[\dfrac{n}{2^{k+1}}+\dfrac{1}{2}\right]$.

当$a_k=0$时为$(a_ma_{m-1}\cdots a_{k+1})$,当$a_k=1$时为$(a_ma_{m-1}\cdots a_{k+1}+a_k)_2$,总之可归于后者.故

$$\begin{aligned}\sum_{k=0}^{\infty}\left[\frac{n+2^k}{2^{k+1}}\right]&=\sum_{k=0}^{m}(a_m\cdots a_{k+1})_2+\sum_{k=0}^{m+1}(a_k)_2=(a_ma_{m-1}\cdots a_1+a_ma_{m-1}\cdots a_2+\cdots+a_ma_{m-1}+\\&\quad a_m)_2+(a_0+a_1+\cdots+a_{m-1}+a_m)_2\\&=a_0+a_1(1+1)_2+a_2(1+1+10)_2+\cdots+a_m(1+1+10+\cdots+1\underbrace{00\cdots0})_2\\&=(a_ma_{m-1}\cdots a_1a_0)_2=n\text{为所求.}\end{aligned}$$

8. 只要称4次就一定可以把少装的一箱找出来. 把15箱产品依次编号为1,2,…,15,再把1~15用二进制表示得一表(略).

易知1~15的数用二进制表示需要4位数,把每位数中出现"1"的箱号归并在一起,就可以得4个组为:1,3,5,7,9,11,13,15;2,3,6,7,10,11,14,15;4,5,6,7,12,13,14,15;8,9,10,11,12,13,14,15.

对每一组中的箱子集中来称一次,如果重量正常记作0,如果重量轻了记作1,共称4次,这时得到一个二进制表示的数:$x=(\overset{④}{\times}\overset{③}{\times}\overset{②}{\times}\overset{①}{\times})_2$就是少装产品的一箱的箱号. 例如,称的结果是第①组和第③组轻了,则$x=(0101)_2=5$,说明轻的一箱(即少装产品的一箱)一定是第5号箱子.

9. 由于 $1990=2^{10}+2^9+2^8+2^7+2^6+0\cdot2^5+0\cdot2^4+0\cdot2^3+2^2+2^1+0\cdot2^0$，且把 1，2，…，1989 也写成 2 进制的形式，操作如下：

第一次，在够取的堆中各取走 $2^{10}=1024$ 块石头；第二次在够取的堆中各取走 $2^9=512$ 块，…，最后，取走仅剩 $2^0=1$ 块的那些堆中的石头，这样，总共用了 11 次，因为含一块石头的堆，故必有取一块石头的操作，如余下的操作取走都是超过 2 块，则恰有两块的堆无法取走，故 2 次操作最多取 $1+2=3$ 块，…，10 次操作最多取走 $1+2+2^2+\cdots+2^9=1023$ 块，因而 1990 堆石头至少要进行 11 次操作.

10. 设所求的数为 A. 在七进制中，A 可写为 $A=7^2\cdot a+7\cdot b+c$，这里 a，b，$c\in\{0,1,2,3,4,5,6\}$，$a\neq0$.

数 A 在九进制中可表示为 $A=9^2\cdot c+9\cdot b+a$.

于是由题意得方程 $7^2\cdot a+7\cdot b+c=9^2\cdot c+9\cdot b+a$，即 $b=8(3a-5c)$.

于是 b 是 8 的倍数，又 $b\in\{0,1,2,\cdots,6\}$，则只能有 $b=0$.

再由 $3a-5c=0$ 及 a，$c\in\{0,1,2,\cdots,6\}$，$a\neq0$，可得 $a=5$，$c=3$.

于是数 A 在七进制中为 $(503)_7$，在九进制中为 $(305)_9$，在十进制中为 $A=7^2\cdot5+3=248$.

11. 考虑多项式 $b\cdot5^4+c\cdot5^3+d\cdot5^2+e\cdot5+f=625b+125c+25d+5e+f$，其中每个字母表示用其系数相应的毫升数的量杯使用的次数.

如字母取正值，则表示从水缸中量水倒入水桶；如字母取负值，则表示从水桶中量水倒入水缸. 并令 b，c，d，e，f 在 $\{-2,-1,0,1,2\}$ 中取值，则

$$625b+125c+25d+5e+f\leqslant625\cdot2+125\cdot2+25\cdot2+5\cdot2+2=1562.$$

又 $a=625b+125c+25d+5e+f$ 的最小值为 -1562，而从 -1562 到 1562 之间恰有 3125 种取值方法.

同时 $625b+125c+25d+5e+f$ 也有 $5^5=3125$ 种不同取法，所以多项式 $625b+125c+25d+5e+f$ 可以得到 -1562 到 1562 的每一个整数值.

12. 我们只需证得 F_n 被 10 除时余数都为 7 即可. 现归于二进制，只需证明：当 $n\geqslant2$ 时，$(1\underbrace{00\cdots0}_{2^n个}1)_2$ 被 $(1010)_2$ 除时余数恒为 $(111)_2$. 经列竖式二步试除，余数为 $(10)_2$，这说明出现循环，因而被除数中每次除去 4 个零而不改变余数. 现考虑被"压缩"以后的情况. 据所获规律，去零过程，被除数可视为 $(1\underbrace{00\cdots0}_{}1)_2$，其中零的个数 m 应取 $m=[(2^n-1)-4k]_{\min}=[4(2^{n-2}-k)-1]_{\min}(k\geqslant0)$. 因题设 $n\geqslant2$，故 $m=3$，而由 $(10001)_2$ 除以 $(1010)_2$，可得余数为 $(111)_2$，即 F_n 的余数恒为 7.

13. 由 $n!$ 中所含素因子 p 的方次数的计算公式，现在取 $p=2$，即知在 $n!$ 中含因子 2 的方次数为

$$\sum_{i=1}^{\infty}\left[\frac{n}{2^i}\right]=\left[\frac{n}{2}\right]+\left[\frac{n}{2^2}\right]+\left[\frac{n}{2^3}\right]+\cdots.$$

充分性. 设 $n=2^{k-1}$，于是

$$\sum_{i=1}^{\infty}\left[\frac{n}{2^i}\right]=\sum_{i=1}^{n}[2^{k-i-1}]=[2^{k-2}]+[2^{k-3}]+\cdots+[2]+[1]$$

$=1+2+2^2+\cdots+2^{k-2}=2^{k-1}-1=n-1.$

这说明在 $n!$ 中含 2 的方次数为 $n-1$,即 $2^{n-1}\mid n!$.

必要性. 设 $2^{n-1}\mid n!$,这必须在 $n!$ 中 2 的方次数$\geqslant n-1$,即 $\sum\limits_{i=1}^{n}\left[\dfrac{n}{2^i}\right]\geqslant n-1$.

将 n 表示为二进制整数,记 $n=(a_1a_2\cdots a_m)_2$,其中 $a_1=1$,显然

$\left[\dfrac{n}{2}\right]=[(a_1a_2\cdots a_{m-1}a_m)_2]=(a_1a_2\cdots a_{m-1})_2$,

$\left[\dfrac{n}{2^2}\right]=[(a_1a_2\cdots a_{m-2}a_{m-1}a_m)_2]=(a_1a_2\cdots a_{m-2})_2$,

$\left[\dfrac{n}{2^3}\right]=[(a_1a_2\cdots a_{m-3}a_{m-2}a_{m-1}a_m)_2]=(a_1\cdots a_{m-3})_2$.

$(1a_2\cdots a_{m-1})_2+(1a_2\cdots a_{m-1})_2+\cdots+(1a_2)_2\geqslant(1a_2\cdots a_{m-1}a_m)_2-1$, $\qquad$ (*)

(*)式左边就是$(\underbrace{11\cdots1}_{m-1\text{个}})_2+a_2(\underbrace{1\cdots1}_{m-2\text{个}})_2+\cdots+a_{m-2}(11)_2+a_{m-1}=(2^{m-1}-1)+a_2(2^{m-2}-1)+\cdots+a_{m-2}(2^2-1)+a_{m-1}(2-1)=(1a_2\cdots a_{m-1}a_m)_2-1-(a_2+a_3+\cdots+a_{m-1}+a_m)$.

故原不等式相当于$-(a_2+a_3+\cdots+a_m)\geqslant0$. 这只有 $a_2=a_3=\cdots=a_m=0$ 时才有可能.

这就是说,$n=(1\underbrace{00\cdots0}_{m-1\text{个}0})_2$,用十进制表示就是 $n=2^{m-1}$.

14. n 表示为 $n=2^tq$,其中 q 为奇数,则

$m^n-1=m^{2^tq}-1=(m^{2^t})^q-1$

$\qquad=(m^{2^t}-1)[(m^{2^t})^{q-1}+(m^{2^t})^{q-2}+\cdots+m^{2^t}+1]$

$\qquad=(m^{2^t}-1)A$,其中 $A\equiv1(\mathrm{mod}\ 2)$.

于是 $2^{1989}\mid(m^n-1)\Leftrightarrow2^{1989}\mid(m^{2^t}-1)$.

因此,可设 $n=2^t$,这时有两种情况:

(1) 若 $m\equiv1\ (\mathrm{mod}\ 4)$,则 m 的二进制表示为 $m=\underbrace{1\cdots100\cdots01}_{k\text{个数字}}$,即 k 是使 $m\equiv1\ (\mathrm{mod}\ 2^k)$ 的最大整数,于是 $m^2-1=(m+1)(m-1)$被 2^{k+1} 整除而不被 2^{k+2} 整除. 设 $m^{2^t}-1$ 被 2^{k+t} 整除而不被 2^{k+t+1} 整除,则 $m^{2^{t+1}}-1=(m^{2^t}+1)(m^{2^t}-1)$被 2^{k+t+1} 整除,而不被 2^{k+t+2} 整除.

所以对所有自然数 s,$2^{s+k}\mid(m^{2^s}-1)$,$2^{s+k+1}\nmid(m^{2^s}-1)$.

(2) 若 $m\equiv3(\mathrm{mod}\ 4)$,则 m 的二进制表示为 $m=\underbrace{1\cdots011\cdots1}_{k\text{个数字}}$,即 k 为使 $m\equiv-1(\mathrm{mod}\ 2^k)$成立的最大整数,同样可证对所有自然数 s,$2^{s+k}\mid(m^{2^s}-1)$,$2^{s+k+1}\nmid(m^{2^s}-1)$.

于是,由 $2^{1989}\mid(m^{2^s}-1)\Rightarrow1989\leqslant s+k\Rightarrow s\geqslant1989-k$($k$ 的定义见上面).

因而在 $k\leqslant1989$ 时,最小的指数 $n=2^{1989-k}$,在 $k>1989$ 时,$n=2^0=1$.

15. 20000 在 31 进制表示中为 $20000=20\cdot31^2+25\cdot31+5$.

所以小于 20000 的数,在 31 进制中的数字和不大于 $19+30+30=79$.

如果素数 $p<20000$,而 $p=a_2\cdot31^2+a_1\cdot31+a_0=a_2\cdot960+a_1\cdot30+(a_2+a_1+a_0)$,则 $a_2+a_1+a_0\leqslant79$.

由于 p 为素数,所以 $a_2+a_1+a_0$ 不能被 2,3,5 整除,否则,若 $a_2+a_1+a_0$ 能被 2,3,5 之

一整除，由于 $30\mid a_2\cdot 960$，$30\mid a_1\cdot 30$，则 p 能被 2，3，5 之一整除，这是不可能的.

在不大于 79 且不能被 2，3，5 整除的合数中只有两个，即 $49=7\cdot 7$ 和 $77=7\cdot 11$.

容易验证 $619=19\cdot 31+30$，$709=22\cdot 31+27$，$739=23\cdot 31+26$，$18257=18\cdot 31^2+30\cdot 31+29$ 等素数在 31 进制中的数字和为 49 或 77.

16. 由 a 进制的定义

$A_{n-1}=x_{n-1}a^{n-1}+x_{n-2}a^{n-2}+\cdots+x_1a+x_0$，$A_n=x_na^n+x_{n-1}a^{n-1}+\cdots+x_1a+x_0$，其中 $a>1$.

所以有

$$\frac{A_{n-1}}{A_n}=1-\frac{x_na^n}{x_na^n+x_{n-1}a^{n-1}+\cdots+x_1a+x_0}$$

$$=1-\frac{x_n}{x_n+x_{n-1}\cdot\frac{1}{a}+\cdots+x_1\cdot\frac{1}{a^{n-1}}+x_0\cdot\frac{1}{a^n}}.$$

同理有 $\frac{B_{n-1}}{B_n}=1-\frac{x_n}{x_n+x_{n-1}\cdot\frac{1}{b}+\cdots+x_1\cdot\frac{1}{b^{n-1}}+x_0\cdot\frac{1}{b^n}}$.

因为 $a>b>1$，则 $\frac{1}{a}<\frac{1}{b}$，并且 $x_n\neq 0$，$x_{n-1}\neq 0$，所以有

$$x_n+x_{n-1}\cdot\frac{1}{a}+\cdots+x_1\cdot\frac{1}{a^{n-1}}+x_0\cdot\frac{1}{a^n}<x_n+x_{n-1}\cdot\frac{1}{b}+\cdots+x_1\cdot\frac{1}{b^{n-1}}+x_0\cdot\frac{1}{b^n},$$

从而 $\frac{x_n}{x_n+x_{n-1}\cdot\frac{1}{a}+\cdots+x_1\cdot\frac{1}{a^{n-1}}+x_0\cdot\frac{1}{a^n}}>\frac{x_n}{x_n+x_{n-1}\cdot\frac{1}{b}+\cdots+x_1\cdot\frac{1}{b^{n-1}}+x_0\cdot\frac{1}{b^n}}$.

于是 $\frac{A_{n-1}}{A_n}<\frac{B_{n-1}}{B_n}$.

17. 设 T 是这样的正整数集合，它的元素在三进制表示中最多有 11 位数字，且每一位的数字都是 0 或 1，但不全为 0. 这样的正整数显然有 $2^{11}-1>1983$ 个，并且 T 中的最大数是 $1+3+3^2+\cdots+3^{10}=88573<10^5$.

为此，我们选择 T 中的 1983 个数，下面证明 T 中任何三数都不是某个等差数列中的连续三项，否则，若 x，y，$z\in T$，且 $x+z=2y$，此时 $2y$ 的三进制表示中必只含数字 0 和 2，从而 x 和 z 一定是所有对应位的数字都相同，即 $x=z$，这是不可能的.

综上，我们证明了确能选择 1983 个不同的正整数，使它们都不大于 10^5，且其中任何三数都不是某等差数列中的连续三项.

18. 考虑 1985 的三进制表示 $1985=2\cdot 3^6+2\cdot 3^5+3^3+3^2+3+2$.

但是，由题设，表示式中的系数不能是 2，而 $2=3-1$，则 1985 可表示为

$1985=3^7-3^5+3^4-3^3-3^2-3-1$. 同样有 $1984=3^7-3^5+3^3+3^2+3+1$.

现在从 1984 开始，逐步减 1，可能出现两种情况：

一种是像 1984 这样的数，后面的若干项是正的，可以减 1，项数不会增；另一种是像 1985 这样的数，最后若干项是负数，减去 1 就会出现 $-2\cdot 3^i$（$i=0,1,2,3$），这样由于 $-2\cdot 3^i=-3^{i+1}+3^i$，把 $-2\cdot 3^i$ 换成 $-3^{i+1}+3^i$，虽然多了一项，由于 1985 的表达式只有 7 项，所以多了一项之后也不会多于 8 项，而当 $i+1=4$ 或 7 时，与原来前面的正项正好抵消，从而项数保持

不变.

所以对于 $k\in[0,\ 1985]$ 中的数都能用 $k=\sum\limits_{i=1}^{k}a_i3^{i-1}, a_i\in\{-1,0,1\}$ 表示.

若把式中的 a_i 换成它的相反数，则对于 $k\in[-1985,\ 0]$ 也可用上式表示.

于是，题目所求的 $n_i=3^{i-1}$，$i=1,\ 2,\ \cdots,\ 8$.

19. 我们把 0 也看作是“坏数”，这样并不影响所求的结果. 先用数学归纳法证明引理：在 0 到 2^n-1 ($n\geqslant 2$) 中，“坏数”的个数与和都恰好占了它们的一半.

(1) 在 0 到 2^2-1 中，即在 0，1，2，3 中，0 是“坏数”，$3=(11)_2$ 是“坏数”，所以有 2 个“坏数”，且$0+3=\frac{1}{2}(0+1+2+3)$,所以在 0 到 2^2-1 中，“坏数”的个数是它们的一半，其和也是它们的和的一半.

(2) 假设在 0 到 2^n-1 中，“坏数”的个数与和都恰好等于它们的一半.

由于把到 2^n-1 中的每个数都加上 2^n，就相当于在二进制数中多了一个 1，因此，0 到 2^n-1 中的“坏数”都变成了“非坏数”，从而 $0+2^n$ 到 2^n-1+2^n 即 a^n 到 $2^{n+1}-1$ 中“坏数”的个数与和也恰好为它们的一半，因此，0 到 $2^{n+1}-1$ 中“坏数”的个数与和都恰好占了一半.

这样就用数学归纳法证明了引理.

于是，从 0 到 2^n-1 中“坏数”的个数为 2^{n-1} 个，它们的和为$\frac{1}{2}[1+2+\cdots+(2^n-1)]=2^{n-2}(2^n-1)$.

由于 $1984=2^{10}+2^9+2^8+2^7+2^6$,而前 2^{10} 个“坏数”的和为 $2^9(2^{11}-1)$,

前$(2^{10}+2^9)$个“坏数”的和还要加上 2^{11} 到 $2^{11}+2^{10}-1$ 中“坏数”的和,即 $2^{11}\cdot 2^9+2^8(2^{10}-1)$.

由此,前 $2^{10}+2^9+2^8+2^7+2^6=1984$ 个“坏数”,还要再加上$(2^{11}+2^{10})\cdot 2^8+2^7(2^9-1)+(2^{11}+2^{10}+2^9)\cdot 2^7+2^6(2^8-1)+(2^{11}+2^{10}+2^9+2^8)\cdot 2^6+2^5(2^7-1)$.

于是前 1986 个“坏数”(包括 0,若不包括 0 即为前 1985 个“坏数”)的和为

$$2^9(2^{11}-1)+2^{11}\cdot 2^9+2^8(2^{10}-1)+(2^{11}+2^{10})\cdot 2^8+2^7(2^9-1)+(2^{11}+2^{10}+2^9)\cdot 2^7+$$
$$2^6(2^8-1)+(2^{11}+2^{10}+2^9+2^8)\cdot 2^6+2^5(2^7-1)+(2^{11}+2^{10}+2^9+2^8+2^7)\cdot 2+2+1$$
$$=2^{21}+2^{20}+2^{19}+2^{18}+2^{13}+2^{11}+2^9+2^8+2^5+2+1.$$

这就是所求的前 1985 个“坏数”的和（十进制).

习题 B

1. 考察数$\overline{xyz}$,满足 $100x+10y+z=30(x+y+z)$.

如果一个整数是 30 的倍数,则其最后一位为 0,故数字 z 必为 0. 于是,有

$100x+10y=30(x+y)$,即 $10x+y=3(x+y)$.

从而,有 $7x=2y$.

由于 x,y 都是一位数字,仅有的可能是 $x=2,y=7$,于是,只存在一个三位数,它等于它的各位数字之和的 30 倍,这个数是 270.

2. 令 $a=100a_3+10a_2+a_1$,

$b=100b_3+10b_2+b_1$,

$c=100c_3+10c_2+c_1$,

$(1\leqslant a_3,b_3,c_3\leqslant 9,0\leqslant a_2,b_2,c_2,a_1,b_1,c_1\leqslant 9)$.

设 $i=a_1+b_1+c_1,j=a_2+b_2+c_2,k=a_3+b_3+c_3$.

由题设有 $i+10j+100k=2005$,且 $i,j,k\leqslant 27$.故 $(i,j,k)=(5,0,20),(5,10,19),(5,20,18),(15,9,19),(15,19,18),(25,8,19),(25,18,18)$.

因此,当 $(i,j,k)=(25,18,18)$ 时,

$S(a)+S(b)+S(c)=i+j+k$ 是最大的.

当 $i=25$ 时,(a_1,b_1,c_1) 的可能对是 $(7,9,9),(8,8,9)$ 及它们的置换,所以,有 $3\times 2=6$ 个可能对.

当 $j=18$ 时,(a_2,b_2,c_2) 的可能对是 $(0,9,9),(1,8,9),(2,7,9),(2,8,8),(3,6,9),(3,7,8),(4,5,9),(4,6,8),(4,7,7),(5,5,8),(5,6,7),(6,6,6)$ 及它们的置换,所以,有 $6\times 7+3\times 4+1=55$ 个可能对.

当 $k=18$ 时,(a_3,b_3,c_3) 的可能对是 (a_2,b_2,c_2) 的那些对,但 $(0,9,9)$ 及其置换必须除掉,所以,有 $55-3=52$ 个 (a_3,b_3,c_3) 的可能对.

因此,满足条件的 (a,b,c) 的个数是

$6\times 55\times 52=17160$.

3. $f(x)=f(0.b_1b_2b_3\cdots)=0.b_1b_1b_2b_2b_3b_3\cdots$.设 $x=0.b_1b_2b_3\cdots$,其中 $b_i=0$ 或 1(对每个 i).

如果 $b_1=0$,则二进制表示的数

$x=0.0b_2b_3b_4\cdots$.

所以,用十进制表示的数 x 为

$$x=0+0\times 2^{-1}+b_2\cdot 2^{-2}+b_3\cdot 2^{-3}+b_4\cdot 2^{-4}+\cdots$$

$$=\frac{b_2}{4}+\frac{b_3}{8}+\frac{b_4}{16}+\cdots \qquad ①$$

$$\leqslant\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\cdots<\frac{1}{2}.$$

因为 $x<\frac{1}{2}$,由①得

$$2x=\frac{b_2}{2}+\frac{b_3}{2^2}+\frac{b_4}{2^3}+\cdots.$$

而 $2x$ 的二进制表示为 $0.b_2b_3b_4\cdots$,

因此,$f(x)=\frac{f(2x)}{4}=\frac{1}{4}f(0.b_2b_3b_4\cdots)=0.b_1b_1+\frac{1}{4}f(0.b_2b_3b_4\cdots)$. ②

若 $b_1=1$,则二进制表示的数 $x=0.1b_2b_3b_4\cdots$,于是,十进制表示的数

$$x=\frac{1}{2}+\frac{b_2}{2^2}+\frac{b_3}{2^3}+\frac{b_4}{2^4}+\cdots\geqslant\frac{1}{2}.$$

所以,$f(0.1b_2b_3b_4\cdots)=f(x)=\frac{3}{4}+\frac{f(2x-1)}{4}$.

另一方面，$x=\frac{1}{2}+\frac{b_2}{2^2}+\frac{b_3}{2^3}+\frac{b_4}{2^4}+\cdots$，则

$$2x-1=\left(1+\frac{b_2}{2^1}+\frac{b_3}{2^2}+\frac{b_4}{2^3}+\cdots\right)-1=\frac{b_2}{2}+\frac{b_3}{2^2}+\frac{b_4}{2^3}+\cdots.$$

而 $2x-1$ 的二进制表示为 $0.b_2b_3b_4\cdots$，

所以，有

$$f(0.1b_2b_3b_4\cdots)=\frac{3}{4}+\frac{1}{4}f(0.b_2b_3b_4\cdots)=\left(\frac{1}{2}+\frac{1}{2^2}\right)+\frac{1}{4}f(0.b_2b_3b_4\cdots)$$

$$=0.b_1b_1+\frac{1}{4}f(0.b_2b_3b_4\cdots). \quad ③$$

由②③得

$$f(x)=f(0.b_1b_2b_3\cdots)=0.b_1b_1+\frac{1}{4}f(0.b_2b_3b_4\cdots).$$

类似地，可得

$f(x)=0.b_1b_1+0.00b_2b_2+0.0000b_3b_3+\cdots=0.b_1b_1b_2b_2b_3b_3\cdots$.

4. 用 $f(X)$ 表示有限数集 X 中元素的算术平均.

(1) 证明：存在 n 个不同正整数构成的集合 S_1，使得对 S_1 的任意两个不同的非空子集 A,B，数 $f(A)$ 和 $f(B)$ 是不相等的正整数.

事实上，取定一个整数 $q>n$，设

$S_1=\{n!\ q,n!\ q^2,\cdots,n!\ q^n\}$.

则对 S_1 的任一个非空子集 A，数 $f(A)$ 显然是一个正整数.

假设存在 S_1 的两个不同的非空子集 A，B，使得 $f(A)=f(B)$.

那么，$|B|\sum\limits_{n!q^i\in A}q^i=|A|\sum\limits_{n!q^j\in B}q^j$.

因为 $q>n\geqslant\max\{|A|,|B|\}$，所以，

$|B|\sum\limits_{n!q^i\in A}q^i=\sum\limits_{n!q^i\in A}|B|q^i$ 与 $|A|\sum\limits_{n!q^j\in B}q^j=\sum\limits_{n!q^j\in B}|A|q^j$

均为正整数的 q 进制表示．从而，它们的形式应当完全相同．由此得 $|A|=|B|$，及 $A=B$，矛盾.

因此，对 S_1 的任意两个不同的非空子集 A，B，数 $f(A)$ 和 $f(B)$ 必定不等.

(2) 设 k 是一个固定的正整数，$k>\max\limits_{A_1\subseteq S_1}f(A_1)$. 证明：对任何正整数 x，正整数的 n 元集合 $S_2=\{k!xa+1\mid a\in S_1\}$ 具有下述性质：对 S_2 的任意两个不同的非空子集 A,B，数 $f(A)$ 和 $f(B)$ 是两个互素的整数.

事实上，由 S_2 的定义易知，对 S_2 的任意两个不同的非空子集 A,B，相应地有 S_1 的两个子集 A_1,B_1，满足

$|A_1|=|A|,|B_1|=|B|$，且

$$f(A)=k!xf(A_1)+1,f(B)=k!xf(B_1)+1. \quad ①$$

显然，$f(A)$ 和 $f(B)$ 都是正整数.

设正整数 d 是 $f(A)$ 与 $f(B)$ 的一个公约数，则 $f(A)f(B_1)-f(B)f(A_1)$ 是 d 的倍数.

故由式①可知 $d|(f(A_1)\quad f(B_1))$.

但由 k 的选取及 S_1 的构作可知，$|f(A_1)-f(B_1)|$ 是小于 k 的非零整数，故它是 $k!$ 的约数，从而，$d|k!$.

再结合 $d|f(A)$ 及式①知，$d|1$，故 $d=1$.

从而，$f(A)$ 与 $f(B)$ 互素.

(3) 证明：可选择正整数 x，使得 S_2 的每个非空子集的元素平均值都是合数.

由于素数有无穷多个，故可选择 2^n-1 个互不相同且均大于 k 的素数 $p_1,p_2,\cdots,p_{2^n-1}$. 将 S_1 中每个非空集合的元素平均值记为 $a_1,a_2,\cdots,a_{2^n-1}$，则

$(p_i,k!a_i)=1(1\leqslant i\leqslant 2^n-1)$，且 $(p_i^2,p_j^2)=1(1\leqslant i<j\leqslant 2^n-1)$.

故由中国剩余定理可知，同余方程组

$k!\ xa_i\equiv -1(\mathrm{mod}\ p_i^2)(i=1,2,\cdots,2^n-1)$ 有正整数解.

任取这样一个解 x，则相应的集合 S_2 的每个非空子集的元素的平均值都是合数.

结合 (2) 的结果，这一 n 元集合满足问题的全部要求.

5. 在以下所讨论的 $K(n,m)$ 中，规定 $m\geqslant n$.

易知 $K(0,m)=\varnothing$，$n\in K(n,m)$.

先列出若干项，从中寻找规律.

$K(1,m)=\{1\}$，$K(2,m)=\{2\}$；

$K(3,m)=\{1,2,3\}$，$K(4,m)=\{4\}$；

$K(5,m)=\{1,4,5\}$，$K(6,m)=\{2,4,6\}$，

$K(7,m)=\{1\sim 7\}$，$K(8,m)=\{8\}$；

$K(9,m)=\{1,8,9\}$，$K(10,m)=\{2,8,10\}$，

$K(11,m)=\{1,2,3,8,9,10,11\}$，

$K(12,m)=\{4,8,12\}$，

$K(13,m)=\{1,4,5,8,9,12,13\}$，

$K(14,m)=\{2,4,6,8,10,12,14\}$，

$K(15,m)=\{1\sim 15\}$，$K(16,m)=\{16\}$.

经计算及定义知 $K(n,m)$ 只与 n 有关，与 m 无关.

下面用数学归纳法证明两个引理.

引理 1　$K(2n,m)=\{2j|j\in K(n,m)\}$.

引理 1 的证明：　假设命题对小于 n 的正整数成立.

用归纳法可证 $1\in K(2n-1,m)$，$1\notin K(2n,m)$，$n\in\mathbf{N}_+$，所以，$2j+1\notin K(2n,m)$.

又 $2j\in K(2n,m)\Leftrightarrow K(2j,m)\cap K(2n-2j,m)=\varnothing$

$\Leftrightarrow K(j,m)\cap K(n-j,m)=\varnothing$(由归纳假设)

$\Leftrightarrow j\in K(n,m)$.

引理 2　$K(2^n+i,m)=\{2^n+i\}\cup K(i,m)\cup\{2^n+i-j|j\in K(i,m)\}$，　①

其中 $1\leqslant i<2^n$.

引理 2 的证明：　假设式①对小于 2^n+i 的正整数成立.

对于任意 $j\in K(i,m)$,若 $j<i$,则

$K(j,m)\cap K(i-j,m)=\varnothing$

$\Rightarrow K(j,m)\cap K(2^n+i-j,m)=\varnothing$(由归纳假设)

$\Rightarrow j\in K(2^n+i,m)$.

若 $j=i$,由 $i\in K(i,m)$,$K(j,m)\cap\{2^n\}=\varnothing$,即 $K(i,m)\cap K(2^n,m)=\varnothing\Rightarrow i\in K(2^n+i,m)$.

所以,$K(i,m)\subset K(2^n+i,m)$.

由定义知 $\{2^n+i-j\mid j\in K(i,m)\}\subset K(2^n+i,m)$,$2^n+i\in K(2^n+i,m)$.

综上,式①右边集合 $\subseteq K(2^n+i,m)$.

对于任意 $j\in K(2^n+i,m)$,由定义,不妨设 $j<\frac{2^n+i}{2}$.若 $j\leqslant i$,则

$K(j,m)\cap K(2^n+i-j,m)=\varnothing$

$\Rightarrow K(j,m)\cap K(i-j,m)=\varnothing$(由归纳假设)

$\Rightarrow j\in K(i,m)$.

下面证明,当 $i<j<\frac{2^n+i}{2}$ 时,$j\notin K(2^n+i,m)$.

令 $j=i+k$,此时 $k<2^{n-1}$,只须证

$K(i+k,m)\cap K(2^n-k,m)\neq\varnothing$.

由式①知,对任意 $k<2^n$,对比二进制,记 $k=\sum\limits_{s=1}^{r}2^{a_s}$,其中 $0\leqslant a_1<a_2<\cdots<a_r$,则

$\{2^{a_s}\mid s=1,2,\cdots,r\}\subset K(k,m)$.

若 $i+k$ 在二进制下不进位,则

$2^{a_1}\in K(i+k,m)\cap K(k,m)\cap K(2^n-k,m)$.

若 $i+k$ 在二进制下进位,设其在第 t 位最后一次进位,由 $j<\frac{2^n+i}{2}$,知 $t<n$,则 i,k 在 2^t 的系数为 0,$i+k$ 在 2^t 的系数为 1.此时,2^n-k 在 2^t 的系数为 1,故 $2^t\in K(i+k,m)\cap K(2^n-k,m)$.

下面解答原题.由引理 1,2,知

$$
\begin{aligned}
|K(2004,m)|&=|K(1002,m)|=|K(501,m)|=|K(256+245,m)|\\
&=2|K(245,m)|+1=2|K(128+117,m)|+1\\
&=4|K(117,m)|+3=4|K(64+53,m)|+3\\
&=8|K(53,m)|+7=8|K(32+21,m)|+7\\
&=16|K(21,m)|+15=16|K(16+5,m)|+15\\
&=32|K(5,m)|+31=32\times 3+31=127.
\end{aligned}
$$

所以,集合 $K(2004,2004)$ 中的元素个数为 127.

6. (1) 对于任意正整数 m,存在非负整数 k 和 l,使得 $2^n\leqslant m<2^l$,则 m 是 2^l-2^n 个数的算术平均,其中有 $m-2^n$ 个数是 2^l,2^l-m 个数是 2^n,即

$$\frac{1}{2^l-2^n}[2^l(m-2^n)+2^n(2^l-m)]=m.$$

所以,m 是"好数".

(2) 假设整数 m 是"坏数",对于任意正整数 k,若 $m\times 2^k$ 不是坏数,则存在 $k_1<k_2<\cdots<k_n$,使得

$$m\times 2^k=\frac{2^{k_1}+2^{k_2}+\cdots+2^{k_n}}{n}.$$

所以 $m\times 2^k=\frac{2^{k_1}(1+2^{l_2}+\cdots+2^{l_n})}{n}$,其中 $l_i=k_i-k_1$,$i=2,3,\cdots,n$.

由于 $1+2^{l_2}+\cdots+2^{l_n}$ 为奇数,则 $k_1\geqslant k$,所以,

$$m=\frac{2^{k_1-k}(1+2^{l_2}+\cdots+2^{l_n})}{n}.$$

这表明,m 是 n 个数 $2^{k_1-k},2^{k_2-k},\cdots,2^{k_n-k}$ 的算术平均,与 m 是坏数矛盾.

因此,只要找到一个坏数即可.

下面证明 13 是坏数.

假设 13 是 n 个 2 的整数次幂的算术平均,于是,$13n$ 在二进制下有 n 个 1.

当 $n=1,2,\cdots,6$ 时,有

$13\times 1=1101_{(2)}$,

$13\times 2=26=11010_{(2)}$,

$13\times 3=39=100111_{(2)}$,

$13\times 4=52=110100_{(2)}$,

$13\times 5=65=1000001_{(2)}$,

$13\times 6=39\times 2=1001110_{(2)}$.

当 $n\geqslant 7$ 时,有 $13n<2^n-1$,所以,

$13n<1+2+2^2+\cdots+2^{n-1}$.

于是,当 $n\geqslant 7$ 时,$13n$ 在二进制下 1 的数目不可能等于 n. 所以,13 是坏数.

因此,所有形如 13×2^n 的数都是坏数.

7. 首先证明:2 的幂有任意长的零区间.

显然,在 2^n 的十进制表示中至少有 k 个连续的 0,当且仅当 2^n 具有

$y\cdot 10^{m+k}+z$

的形式,其中 y,z 是正整数,且 z 至多有 m 位,即

$z<10^m$.

故只须证明:存在 n 和 m,满足 2^n 模 10^{m+k} 的余数小于 10^m.

根据欧拉定理,对每个正整数 t,因 $(2,5^t)=1$,故有

$2^{\varphi(5^t)}\equiv 1(\mathrm{mod}\ 5^t)$,

乘 2^t 得 $2^{t+\varphi(5^t)}\equiv 2^t(\mathrm{mod}\ 10^t)$.

因此,对某个正整数 y,有

$2^{t+\varphi(5^t)}=y\cdot 10^t+2^t$.

根据上述,规定

$n=t+\varphi(5^t)$,$m=t-k$.

令 $2^t<10^{t-k}$,这样的 t 值一定存在. 例如,$t=2k$(因为 $2^{2k}=4^k<10^k$). 由此得,在

$$2^{2k+\varphi(5^{2k})}=y\cdot 10^{2k}+2^{2k}$$

中至少有 k 个 0 的单元.

对于给定的 k，选定 2 的幂（比如 2^n）恰好含有 r 个 0 的单元，其中，$r\geqslant k$.

下面讨论，当用 2 乘这个带零单元的数时，对于某些非零数字 a,b，有

$$2^n=\cdots a\underbrace{0\cdots0}_{r\text{个}}\underbrace{b\cdots}_{s\text{位}}=y\cdot 10^{r+s}+z.$$

因此，$2^{n+1}=2y\cdot 10^{r+s}+2z$.

数 $2z$ 与 z 或者有相同位数的数字，或者多一位. 所以，在零单元的“右边”没有削减或削减一个 0；在零单元“左边”只有当 y 能被 5 整除时才能扩展一个 0.

综上，当 y 不能被 5 整除时，零单元的长度或者减 1，或者不变，且当反复地乘 2 时，每一次零单元的长度至多减少 1.

于是，避免 k 长度零单元的唯一可能是保留大于 k 的长度，但这是不可能的.

设 $y=5^a t$，其中 t 不能被 5 整除.

当用 2 乘 2^n 第 $a+1$ 次时，零单元左边不再扩展，而每乘一个 2 的 4 次幂时零单元右边削减（因 $2^4>10$）. 因此，次数足够后，可以得到恰有 k 个 0 的 2 的幂.

8. 为证原题先证明两个引理.

引理 1　记 $t(t\in\mathbf{Z}_+)$ 的二进制表示中 1 的个数为 $P(t)$，则 $t!$ 中因子 2 的个数为 $(t-P(t))$ 个.

引理 2　$P(t)+P(r)=P(r+t)$，当且仅当 r 与 t 的二进制表示中，任何两个 1 所在的位数不同.

引理 1 的证明：　设 $t=\sum\limits_{i=0}^{n}a_i2^i$，其中 $a_i\in\{0,1\}$，$\sum\limits_{i=0}^{n}a_i=P(t)$，则 $t!$ 中因子 2 的个数为

$$\sum_{j=1}^{n}\left[\frac{t}{2^j}\right]=\sum_{j=1}^{n}\sum_{i=j}^{n}a_i2^{i-j}=\sum_{i=1}^{n}\sum_{j=1}^{i}a_i2^{i-j}=\sum_{i=1}^{n}a_i(2^i-1)=t-P(t).$$

引理 2 的证明：　必要性. 显然成立.

充分性.

记 $t=2^{a_1}+2^{a_2}+\cdots+2^{a_{P(t)}}$，

$r=2^{b_1}+2^{b_2}+\cdots+2^{b_{P(r)}}$.

由 C_{t+r}^{t} 为整数，则

$t+r-P(t+r)\geqslant t-P(t)+r-P(r)$.

所以，$P(t)+P(r)\geqslant P(t+r)$.

若存在 $1\leqslant i\leqslant P(t)$，$1\leqslant j\leqslant P(r)$，使 $a_i=b_j$，则

$P(t+r)\leqslant P(t+r-2^{a_i}-2^{b_j})+P(2^{a_i}+2^{b_j})\leqslant P(t)+P(r)-2+1=P(t)+P(r)-1$.

故对任意 $1\leqslant i\leqslant P(t)$，$1\leqslant j\leqslant P(r)$，$a_i\neq b_j$.

下面证明原题.

当 $k\geqslant t$ 时，

$2\nmid C_k^t\Leftrightarrow k-P(k)=t-P(t)+(k-t)-P(k-t)$

$\Leftrightarrow P(k-t)+P(t)=P(k)$

$\Leftrightarrow(k-t)$ 与 t 的二进制表示中没有两个 1 在同一数位上.

设 $n=2^h$（$h\in\mathbf{Z}_+$，h 充分大），有

$t=2^q+\sum\limits_{i=0}^{q-1}a_i2^i$，$A=\{i|a_i=1\}$，

$|A|=P(t)-1$.

则 $2\nmid C_n^k\Leftrightarrow k-t=\sum\limits_{j=1}^{h-q-1}b_j2^{q+j}+\sum\limits_{\substack{i=0\\i\notin A}}^{q-1}c_i2^i$，$b_j$、$c_i\in\{0,1\}$.

所以，$f_t(n)=2^{h-q-1}\times2^{q-[P(t)-1]}=2^{h-P(t)}$.

故 $\dfrac{f_t(n)}{n}=\dfrac{1}{2^{P(t)}}$.

因此，$r=P(t)$ 依赖于 t，与 n 无关.

9. 因为 $\sum\limits_{i=0}^{n}a_ik^i-\sum\limits_{i=1}^{n}a_i\equiv0(\bmod\ (k-1))$，所以

$\sum\limits_{i=0}^{n}a_ik^i\equiv0(\bmod\ (k-1))$ 与 $\sum\limits_{i=0}^{n}a_i\equiv0(\bmod\ (k-1))$

等价. 于是，经过两次运算以后每个数都可以被 $(k-1)^3$ 整除，这是因为第一次运算后的数可以被 $k-1$ 整除，而这个数在 k 进制表示下各位数码的和也可以被 $k-1$ 整除. 从而，第二次运算后的数可以被 $(k-1)^3$ 整除.

设 $a=\overline{a_na_{n-1}\cdots a_0}_{(k)}$，$n\geqslant4$ 或 $a_3\geqslant2$，$n=3$，则

$a-(k-1)^2(a_n+a_{n-1}+\cdots+a_0)$

$\geqslant2[k^3-(k-1)^2]-a_1[(k-1)^2-k]-a_0[(k-1)^2-1]$

$\geqslant2[k^3-(k-1)^2]-(k-1)[2(k-1)^2-k-1]=5k^2-2k-1>0$.

从而，总可得到一个形如 $\overline{a_3a_2a_1a_0}_{(k)}$ 的数，其中，$a_3=1$ 或 0.

于是，下一个数为

$(k-1)^2(a_3+a_2+a_1+a_0)\leqslant(k-1)^2[1+3(k-1)]<4(k-1)^3$.

因此，这个数为

$(k-1)^3$ 或 $2(k-1)^3$ 或 $3(k-1)^3$.

因为 $(k-1)^3=\overline{k-3,2,k-1}_{(k)}$（$k>2$），其下一个数为 $2(k-1)^3$；

$2(k-1)^3=\overline{1,k-6,5,k-2}_{(k)}$（$k>5$），下一个数为 $2(k-1)^3$；

$3(k-1)^3=\overline{2,k-9,8,k-3}_{(k)}$（$k>8$），下一个数为 $2(k-1)^3$.

又当 $k=6$ 时，$3\times5^3=\overline{1423}_{(6)}$，下一个数为 $5^2\times10=2\times5^3$；

当 $k=7$ 时，$3\times6^3=\overline{1614}_{(7)}$，下一个数为 $6^2\times12=2\times6^3$；

当 $k=8$ 时，$3\times7^3=\overline{2005}_{(8)}$，下一个数为 $7^2\times7-7^3$，再下一个数为 2×7^3.

所以，当 $k>5$ 时，从某个数开始，其后面的数全等于 $2(k-1)^3$.

10. 显然 x 是奇数. 记 t 中 2 的幂次为 $V_2(t)$.

若 m 是奇数. 设 $y=x-1$，则

$x^m-1=(y+1)^m-1=y^m+C_m^1y^{m-1}+C_m^2y^{m-2}+\cdots+C_m^{m-1}y$.

其中 $C_m^{m-1}y$ 项中 2 的幂次为 y 中 2 的幂次，其余项均满足

$V_2(C_m^i y^i)=V_2(y)+(i-1)V_2(y)+V_2(C_m^i)>V_2(y)$.

故 $V_2(x^m-1)=V_2(y)=V_2(x-1)$.

又 $V_2(x^m-1)=V_2(2^{2n+1}+2^n)=n$，有

$V_2(x-1)=n$.

则 $2^n\mid(x-1)$.

所以，$x-1\geqslant 2^n$，$x\geqslant 2^n+1$.

而 $x^3\geqslant(2^n+1)^3=2^{3n}+3\times 2^{2n}+3\times 2^n+1>2^{2n+1}+2^n+1=x^m$，

所以，$m<3$.

故 $m=1$. 此时，$x=2^{2n+1}+2^n+1$.

若 m 为偶数，设 $m=2m_0$，则

$(x^{m_0})^2=7\times 2^{2n-2}+(2^{n-1}+1)^2$，即 $(x^{m_0}-2^{n-1}-1)(x^{m_0}+2^{n-1}+1)=7\times 2^{2n-2}$.

若 $n=1$，则 $x^m=2^3+2^1+1=8+2+1=11$ 不是平方数，不可能.

因此，$n\geqslant 2$.

所以，$x^{m_0}-2^{n-1}-1\not\equiv x^{m_0}+2^{n-1}+1\pmod 4$.

又因为它们都是偶数，则它们之一中 2 的幂次为 1. 只有下面四种情形：

$$\begin{cases}x^{m_0}-2^{n-1}-1=14,\\x^{m_0}+2^{n-1}+1=2^{2n-3};\end{cases}\qquad ①$$

$$\begin{cases}x^{m_0}-2^{n-1}-1=2^{2n-3},\\x^{m_0}+2^{n-1}+1=14;\end{cases}\qquad ②$$

$$\begin{cases}x^{m_0}-2^{n-1}-1=7\times 2^{2n-3},\\x^{m_0}+2^{n-1}+1=2;\end{cases}\qquad ③$$

$$\begin{cases}x^{m_0}-2^{n-1}-1=2,\\x^{m_0}+2^{n-1}+1=7\times 2^{2n-3}.\end{cases}\qquad ④$$

由①有 $2^{n-1}+1=2^{2n-4}-7$，即

$2^{n-4}+1=2^{2n-7}$.

解得 $n=4$，$x^{m_0}=23$.

故 $x=23$，$m_0=1$.

由②有 $2^{n-1}+1=7-2^{2n-4}$，即

$2^{n-1}+2^{2n-4}=6$.

因为 $6=4+2$，故无解.

由③有 $2^{n-1}+1=1-7\times 2^{2n-4}$，也不可能.

由④有 $2^{n-1}+1=7\times 2^{2n-4}-1$，即

$2^{n-2}+1=7\times 2^{2n-5}$.

考察二进制表示中 1 的个数，故也不可能.

所以，$(x,m,n)=(2^{2n+1}+2^n+1,1,n)$，$(23,2,4)$.

11. 由于有无穷多个好数，则一定存在一个好数，至少有 $10k+1$ 位数. 设 $c_1,c_2,\cdots,c_{10k+1}$ 是其在十进制表示下连续的 $10k+1$ 个数码，于是，

$$a=10^{k-1}c_1+10^{k-2}c_2+\cdots+10c_{k-1}+c_k \text{ 和 } b=10^{k-1}c_2+10^{k-2}c_3+\cdots+10c_k+c_{k+1}$$

都是 r 的倍数，则

$10a-b=10^kc_1-c_{k+1}$ 也是 r 的倍数.

设 $d_i=c_{ik+1}(i=0,1,\cdots,10)$.

类似地可得

$r\mid(10^kd_i-d_{i+1})(i=0,1,\cdots,9)$.

由于 $d_0,d_1,\cdots,d_{10}$ 只可以是 $0,1,\cdots,9$ 中的数，则一定存在两项相等，所以，存在 $i,j(0\leqslant i<j\leqslant 10)$，使得 $d_i,d_{i+1},\cdots,d_{j-1}$ 两两不同，且 $d_i=d_j$. 因此，

$$(10^kd_i-d_{i+1})+(10^kd_{i+1}-d_{i+2})+\cdots+(10^kd_{j-1}-d_j)$$
$$=(10^kd_i-d_i)+(10^kd_{i+1}-d_{i+1})+\cdots+(10^kd_{j-1}-d_{j-1})$$
$$=(10^k-1)(d_i+d_{i+1}+\cdots+d_{j-1})$$

可以被 r 整除.

因为 $d_i,d_{i+1},\cdots,d_{j-1}$ 两两不同，所以，$d_i+d_{i+1}+\cdots+d_{j-1}$ 不超过 $0+1+\cdots+9=45$. 可得 $d_i+d_{i+1}+\cdots+d_{j-1}$ 与 r 互素. 因此，10^k-1 可以被 r 整除，即 k 位数 10^k-1 是好数.

12. (1) 由 $a_i\times0+b_i\in C$，得 $b_i\geqslant0$.

若对某些 i，$a_i=1$，则

$C_i=C+b_i\subseteq C$.

由 $0\in C$，得 $0+b_i\in C$，且 $b_i+b_i\in C$，进而对所有非负整数 n，有 $nb_i\in C$.

设 k 是满足 $3^k>b_i$ 的非负整数，则满足 $3^k\leqslant n<2\times3^k$ 的 n 的三进制表示中均含有 1，它们不在 C 中.

而由 $3^k>b_i$，知存在某些 n，使得 nb_i 也包含在这些数中，这与 $nb_i\in C$ 矛盾.

(2) 设非负整数 k 满足 $3^k>b_i$，对任意 $m\in C$，有 $3^km\in C$，则 $3^kma_i+b_i\in C$.

考察 a_im 的三进制表示，并由 $3^k>b_i$，知 $a_im\in C$，于是 $a_iC\subseteq C$.

又 $2\in C$，则 $2a_i\in C$.

故 a_i 的三进制表示中只含有 0，1.

令 $a_i=3^tu(3\nmid u)$.

若 $u=1$，则结论成立. 否则，设 u 的三进制表示中右数第二个 1 的位数为 v. 用 a_i 乘以 $2\times3^{v-1}+2$ 则得到一个 C 之外的数，矛盾.

(3) 设 $a_i=3^k$，并令 $2\times3^l\leqslant b_i\leqslant3^{l+1}$（这是因为 $b_i\in C$ 且其三进制表示中最左端的数码为 2）.

若 $a_i\leqslant b_i$，则 $k\leqslant l$，$2\times3^{l-k}\in C$.

于是 $2\times3^{l-k}a_i+b_i\in C$.

而 $2\times3^{l-k}a_i+b_i$ 的三进制表示的最左端的数码应该是 1，矛盾. 因此，$a_i>b_i$.

(4) 令 $J=\{i\in\{1,2,\cdots,n\}\mid b_i\equiv2(\bmod 3)\}$.

显然，$\varnothing\neq J\neq\{1,2,\cdots,n\}$.

令 $D=\bigcup\limits_{i\in J}C_i$，$E=\bigcup\limits_{i\notin J}C_i$.

容易验证，$D=3C+2$ 且 $E=3C$.

13. 用$[a_1a_2\cdots a_k]_p$表示k位p进制数，将集合M中的每个数乘以7^4，得

$M'=\{a_1\cdot 7^3+a_2\cdot 7^2+a_3\cdot 7+a_4 \mid a_i\in T, i=1,2,3,4\}$

$=\{[a_1a_2a_3a_4]_7 \mid a_i\in T, i=1,2,3,4\}$.

M'中的最大数为$[6666]_7=[2400]_{10}$.

在十进制数中，从2400起从大到小顺序排列的第2005个数是$2400-2004=396$. 而$[396]_{10}=[1104]_7$，将此数除以7^4，便得M中的数是$\frac{1}{7}+\frac{1}{7^2}+\frac{0}{7^3}+\frac{4}{7^4}$. 故选C.

14. 记$\alpha=20042005200620072008$,

$\beta=20042005200620072009$,

为证原命题成立，下面先证明：

引理 对任意$\varepsilon\in(0,1)$，存在$m\in\mathbf{N}^*$，使$0<\{m\lg 2004\}<\varepsilon$.

引理的证明 先证明lg2004是无理数.

反证法：假设存在$p,q\in\mathbf{N}^*$，$(p,q)=1$，使$\lg 2004=\frac{p}{q}$，则$10^p=2004^q$，$p,q\in\mathbf{N}^*$. 但由于$3\nmid 10^p$，$3\mid 2004^q$，因此$10^p\neq 2004^q$，故产生矛盾！假设不成立，所以lg2004是无理数.

由$\varepsilon\in(0,1)$知，存在$n\in\mathbf{N}^*$，使$0<\frac{1}{n}<\varepsilon$. 因此只须证明，存在$m\in\mathbf{N}^*$，使$0<\{m\lg 2004\}<\frac{1}{n}$.

考虑如下$n+1$个数$\{i\lg 2004\}(i=0,1,2,\cdots,n)$及$n$个区间$I_j=\left[\frac{j-1}{n},\frac{j}{n}\right)(j=1,2,\cdots,n)$，由抽屉原理可知必存在一个区间$I_j$，使$\{i_1\lg 2004\},\{i_2\lg 2004\}\in I_j$，$0\leqslant i_1\leqslant i_2\leqslant n+1$.

a) 若$\frac{j-1}{n}\leqslant\{i_1\lg 2004\}\leqslant\{i_2\lg 2004\}<\frac{j}{n}$，则

$0\leqslant\{(i_2-i_1)\lg 2004\}=\{i_2\lg 2004\}-\{i_1\lg 2004\}<\frac{1}{n}$，$i_2-i_1\in\mathbf{N}^*$.

b) 若$\frac{j-1}{n}\leqslant\{i_2\lg 2004\}<\{i_1\lg 2004\}<\frac{j}{n}$，则

$0<\{(i_1-i_2)\lg 2004\}<\frac{1}{n}$,

即 $1-\frac{1}{n}<\{(i_2-i_1)\lg 2004\}<1$.

设 $\{(i_2-i_1)\lg 2004\}=1-\delta$，$0<\delta<\frac{1}{n}$，

则由$0<\delta<\frac{1}{n}$得存在$r\in\mathbf{N}^*$，使$0<1-r\delta<\frac{1}{n}$，于是

$\{r(i_2-i_1)\lg 2004\}=\{r(1-\delta)\}=\{r-1+1-r\delta\}=\{1-r\delta\}\in\left(0,\frac{1}{n}\right)$，$r(i_2-i_1)\in\mathbf{N}^*$.

综合a)、b)知总存在$m\in\mathbf{N}^*$，使$0\leqslant\{m\lg 2004\}<\frac{1}{n}$. 又因为lg2004为无理数，故$\{m\lg 2004\}\neq 0$，所以有$0<\{m\lg 2004\}<\frac{1}{n}$，即引理得证.

下面证明：存在$k,m\in\mathbf{N}^*$，使$k+\lg\alpha\leqslant m\lg 2004<k+\lg\beta$.

显然当取 $d\in(0,1)$ 时，$\lg\alpha\notin\mathbf{Z}$，使 $\lg\alpha+d<\lg\beta$，$\{\lg\alpha\}+d<1$，取 $M\in\mathbf{N}^*$，使 $M\lg2004>\lg\beta+1$. 由引理，存在 $m_0\in\mathbf{N}^*$，使 $0<\{m_0\lg2004\}<\dfrac{d}{M}$，从而 $0<\{Mm_0\lg2004\}<d$. 于是可得存在 $l\in\mathbf{N}^*$，使

$0<\{\lg\alpha\}<l\{m_0M\lg2004\}<\{\lg\alpha\}+d<1$.

另外，由

$\{\lg\alpha\}<\{Mm_0l\cdot\lg2004\}=l\{Mm_0\lg2004\}<\{\lg\alpha\}+d$

$\Leftrightarrow\lg\alpha-[\lg\alpha]+[Mm_0l\cdot\lg2004]<Mm_0l\cdot\lg2004$

$<\lg\alpha-[\lg\alpha]+[Mm_0l\cdot\lg2004]+d$

$<\lg\beta-[\lg\alpha]+[Mm_0l\cdot\lg2004]$.

由此式，若令 $k=[Mm_0l\cdot\lg2004]-[\lg\alpha]$，$m=Mm_0l$，则 $k\in\mathbf{Z}$，$m\in\mathbf{N}^*$，且 $k+\lg\alpha\leqslant m\lg2004<k+\lg\beta$. 由 $m=Mm_0l\geqslant M$，并结合上式知，

$k>m\lg2004-\beta\geqslant M\lg2004-\beta>1$，

从而必有 $k\in\mathbf{N}^*$，$m\in\mathbf{N}^*$，且使命题成立.

由该命题，$\alpha10^k\leqslant2004^m<\beta\cdot10^k$ 可得

$20042005200620072008\cdot10^k\leqslant2004^m<20042005200620072009\cdot10^k$，

从而 2004^m 的十进制位表示开始的数字为 20042005200620072008 的结论成立.

15. 不妨设 $p_1<\cdots<p_{25}$，若 $p_1>2$，由于 2 不能表示成 $(p_1\cdots p_{25})^{2004}$ 的不同正约数之和，故此时 $T=1$.

以下设 $p_1=2$，我们将证明下面更一般的结论：

设 $k\geqslant1$，$p_1,\cdots,p_k$ 为 k 个互不相同的素数，满足 $p_i<p_{i+1}\leqslant p_i^{2005}(i=1,\cdots,k-1)$，$p_1=2$，则能表示成 $(p_1\cdots p_k)^{2004}$ 的不同正约数之和的正整数之集为 $\{1,2,\cdots,T_k\}$，其中

$$T_k=\frac{p_1^{2005}-1}{p_1-1}\cdots\frac{p_k^{2005}-1}{p_k-1}. \quad ①$$

[注意，$(p_1\cdots p_k)^{2004}$ 的所有正约数之和为 T_k.]

我们对 k 归纳来证明：若 $1\leqslant n\leqslant T_k$，则 n 可表示为 $(p_1\cdots p_k)^{2004}$ 的不同正约数之和.

当 $k=1$ 时，设 $1\leqslant n\leqslant T_1=1+2+2^2+\cdots+2^{2004}$，由 n 的二进制表示易知 n 可表示成 2^{2004} 的不同正约数之和.

假设上述结论对 k 成立，设 $1\leqslant n\leqslant T_{k+1}$，由①知 $T_{k+1}=T_k(1+p_{k+1}+\cdots+p_{k+1}^{2004})$，故存在 $i(0\leqslant i\leqslant2004)$，使得

$T_k(p_{k+1}^{i+1}+\cdots+p_{k+1}^{2004})<n\leqslant T_k(p_{k+1}^i+p_{k+1}^{i+1}+\cdots+p_{k+1}^{2004})$

(当 $n=T_{k+1}$ 时，约定上式左端为 0). 故

$$1\leqslant n-T_k(p_{k+1}^{i+1}+\cdots+p_{k+1}^{2004})\leqslant T_kp_{k+1}^i. \quad ②$$

以 p_{k+1}^i 除 $n-T_k(p_{k+1}^{i+1}+\cdots+p_{k+1}^{2004})$ 得

$$n-T_k(p_{k+1}^{i+1}+\cdots+p_{k+1}^{2004})=m_ip_{k+1}^i+r, \quad ③$$

其中 $m_i\geqslant0$，$0\leqslant r<p_{k+1}^i$.

由②，③及 $r\geqslant0$ 易知 $m_i\leqslant T_k$，再由 $r<p_{k+1}^i$ 及③可知，$n-T_k(p_{k+1}^{i+1}+\cdots+p_{k+1}^{2004})-m_ip_{k+1}^i$ 的 p_{k+1} 进制表示必具有下面的形式：

$$n-T_k(p_{k+1}^{i+1}+\cdots+p_{k+1}^{2004})-m_i p_{k+1}^{i}=m_0+m_1 p_{k+1}+\cdots+m_{i-1} p_{k+1}^{i-1},\qquad ④$$

其中 $0\leqslant m_j\leqslant p_{k+1}-1(j=0,1,\cdots,i-1)$. 但由 p_1 [illegible] $1-1$, 及 $p_{u+1}-1\leqslant p_u^{2005}-1$ 对 $u\geqslant 1$, 易知, 对 $j=0,1,\cdots,i-1$ 均有

$$m_j\leqslant p_{k+1}-1\leqslant p_k^{2005}-1\leqslant\frac{p_1^{2005}-1}{p_1-1}\cdot\frac{p_2^{2005}-1}{p_2-1}\cdot\cdots\cdot\frac{p_k^{2005}-1}{p_k-1}=T_k.$$

令 $m_{i+1}=m_{i+2}=\cdots=m_{2004}=T_k$, 则由④及已证的结论知

$$n=m_0+m_1 p_{k+1}+\cdots+m_{2004} p_{k+1}^{2004},\qquad ⑤$$

其中 $0\leqslant m_j\leqslant T_k$, $j=0,1,\cdots,2004$.

由归纳假设, 每一个非零的 m_j 均可表示成 $(p_1\cdots p_k)^{2004}$ 的不同正约数之和, 故由⑤知, n 可表示成 $(p_1\cdots p_k p_{k+1})^{2004}$ 的不同正约数之和. 这就完成了上述结论的归纳证明.

因此, 当 $p_1,\cdots,p_{25}$ 中的最小数大于 2 时, $T=1$; 当最小数为 2 时, $T=\frac{p_1^{2005}-1}{p_1-1}\cdots\frac{p_{25}^{2005}-1}{p_{25}-1}$.

16. 对任意的 $k\in\mathbf{N}_+$, 设 $t=[\log_3 k]$, 分 3 种情形讨论.

(1) 当 $k=3^t$ 时, k 位数 $r_t=\overline{\underbrace{11\cdots1}_{k\text{个}1}}\in A$. 这可利用数学归纳法证明:

首先 $r_0=1\in A$.

其次, 由于 $S(r_{t+1})=3S(r_t)$、$r_{t+1}=\overline{1\underbrace{0\cdots0}_{(3^t-1)\text{个}0}1\underbrace{0\cdots0}_{(3^t-1)\text{个}0}1}\times r_t$, 可被 $3r_t$ 整除知, 在 $r_t\in A$ 时, 有 $r_{t+1}\in A$. 从而 $r_t\in A$ 对一切非负整数 t 成立.

(2) 当 $3^t<k<2\times 3^t$ 时, 设 $l=k-3^t$, k 位数 $u=\overline{\underbrace{1\cdots1}_{(3^t-l)\text{个}0}\underbrace{9\cdots9}_{l\text{个}9}\underbrace{8\cdots8}_{(3^t-l)\text{个}8}}\in A$.

事实上, 由于 $S(u)=9S(r_t)$ 以及 $u=\overline{1\underbrace{0\cdots0}_{(3^t-l-1)}8}\times r_t$, 可被 $9r_t$ 整除, 由 (1) 的结论(注意 u 各位都不为 0)可知 $u\in A$.

(3) 当 $2\times 3^t\leqslant k<3^{t+1}$ 时, 设 $m=k-2\times 3^t$, k 位数 $v=\overline{\underbrace{1\cdots1}_{(2\times3^t-m)\text{个}0}\underbrace{9\cdots9}_{m\text{个}9}\underbrace{8\cdots8}_{(2\times3^t-m)\text{个}8}}\in A$.

事实上, $S(v)=18s(r_t)$, $v=\overline{1\underbrace{0\cdots0}_{(2\times3^t-m-1)}8}\times r_t$, 可被 $18r_t$ 整除, v 各位都不为 0, 由(1)可得结论.

总之, 本题结论成立.

17. 将 n 表示为三进制:

$$n=(a_k a_{k-1}\cdots a_0)_3=a_k\cdot 3^k+\cdots+a_1\cdot 3^1+a_0,$$

其中 $a_j\in\{0,1,2\}$, $j=0,1,2,\cdots,k$, $a_k\neq 0$.

用 A_n 表示 $1,2,\cdots,n$ 的最小公倍数, 则 $A_n=3^k\cdot B_n$, $3\nmid B_n$.

记 $L_n=A_n\cdot\frac{p_n}{q_n}=A_n\left(1+\frac{1}{2}+\cdots+\frac{1}{n}\right)$, 则

$L_n\in\mathbf{N}_+$, 且 $3\mid p_n\Leftrightarrow 3^{k+1}\mid L_n$.

记 $S_j=\sum\limits_{\substack{1\leqslant i\leqslant\frac{n}{3^j}\\ 3\nmid i}}\frac{1}{i}$, $j=0,1,2,\cdots,k$, 则

$$L_n=3^k\cdot B_n\sum_{1\leqslant i\leqslant n}\frac{1}{i}=B_n\cdot S_k+3^1\cdot B_n\cdot S_{k-1}+\cdots+3^k\cdot B_n\cdot S_0.\qquad (*)$$

引理　当 $a_j=0$ 或 2 时，$B_n\cdot S_j\equiv0\pmod 3$；当 $a_j=1$ 时，$B_n\cdot S_j\equiv B_n\pmod 3$.

引理的证明　由于 $\frac{1}{3m+1}+\frac{1}{3m+2}=\frac{3(2m+1)}{(3m+1)(3m+2)}$，故

$B_n\cdot\left(\frac{1}{3m+1}+\frac{1}{3m+2}\right)\equiv0\pmod 3$.

所以当 $a_j=0$ 或 2 时，$B_n\cdot S_j\equiv0\pmod 3$；当 $a_j=1$ 时，$B_nS_j\equiv\frac{B_n}{3r+1}\equiv B_n\pmod 3$.

回到原题，设 $3^{k+1}\mid L_n$. 由(*)得 $B_nS_k\equiv0\pmod 3$.

由引理，知 $a_k=2$，$S_k=\frac{3}{2}$. 若 $k=0$，则 $n=2$.

当 $k\geqslant1$ 时，由(*)得

$0\equiv B_n\cdot\frac{3}{2}+3^1\cdot B_n\cdot S_{k-1}\pmod 9$，则

$0\equiv B_n\cdot S_{k-1}+B_n\cdot\frac{1}{2}\equiv B_n\cdot S_{k-1}-B_n\pmod 3$，故

$B_n\cdot S_{k-1}\equiv B_n\pmod 3$.

由引理知，$a_{k-1}=1$，$S_{k-1}=1+\frac{1}{2}+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}$.

若 $k=1$，则 $n=(2,1)_3=7$.

当 $k\geqslant2$ 时，由(*)得

$0\equiv B_n\cdot\frac{3}{2}+3^1\cdot B_n\cdot S_{k-1}+3^2\cdot B_n\cdot S_{k-2}\pmod{27}$，

则
$$\begin{aligned}0&\equiv3\cdot B_n\cdot S_{k-2}+B_n\cdot\frac{1}{2}+B_n\cdot\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}\right)\\&\equiv3\cdot B_n\cdot S_{k-2}+B_n\cdot\left(2+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}\right)\\&\equiv3\cdot B_n\cdot S_{k-2}+B_n(2-2+2+4)\\&\equiv3\cdot(B_n\cdot S_{k-2}-B_n)\pmod 9,\end{aligned}$$

故　$B_n\cdot S_{k-2}\equiv B_n\pmod 3$.

由引理知，$a_{k-2}=1$，$S_{k-2}=1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{22}$.

若 $k\geqslant3$，由(*)得

$0\equiv B_n\cdot\frac{3}{2}+3^1\cdot B_n\cdot\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}\right)+3^2\cdot B_n\cdot S_{k-2}+3^3\cdot B_n\cdot S_{k-3}\pmod{81}$，

则
$$\begin{aligned}0&\equiv B_n\left(2+\frac{1}{4}+\frac{1}{5}+\frac{1}{7}\right)+3\cdot B_n\cdot S_{k-2}+3^2\cdot B_n\cdot S_{k-3}\\&\equiv B_n(2+7+11+4)+3\cdot B_n\cdot S_{k-2}+3^2\cdot B_n\cdot S_{k-3}\\&\equiv-3\cdot B_n+3\cdot B_n\cdot S_{k-2}+3^2\cdot B_n\cdot S_{k-3}\pmod{27},\end{aligned}$$

从而
$$\begin{aligned}0&\equiv3\cdot B_n\cdot S_{k-3}+B_n\left(-1+1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{22}\right)\\&=3\cdot B_n\cdot S_{k-3}+B_n\left[-1+\left(1+\frac{1}{2}+\frac{1}{4}-\frac{1}{4}-\frac{1}{2}-1\right)\times2+\left(1+\frac{1}{2}+\frac{1}{4}\right)\right]\end{aligned}$$

$\equiv 3\cdot B_n\cdot S_{k-3}+B_n(5-2)$

$\equiv 3\cdot B_n\cdot S_{k-3}+3\cdot B_n \pmod 9$.

故 $B_n\cdot S_{k-3}+B_n\equiv 0 \pmod 3$，由引理知，这不可能.

所以所求的正整数 n 为 2,7 和 22.

第十七章　不定方程

习题 A

1. (1) 两边乘以 4，变形得 $(2x+1)^2+3=4y^2$，即 $(2x+2y+1)(-2x+2y-1)=3$.

假设方程有正整数解 x,y，则 $2x+2y+1>-2x+2y-1$ 均为正整数，所以

$-2x+2y-1=0,2x+2y+1=3$，解之得 $x=0,y=1$，矛盾.

(2) 由于 x 与 $x+1$ 互素，且它们的积是整数的 k 次幂，因此，x 和 $x+1$ 都是正整数的 k 次幂，即

$x=u^k,x+1=v^k,y=uv$.　①

u,v 都是正整数，由①产生 $v^k-u^k=1$，即 $(v-u)(v^{k-1}+v^{k-2}u+\cdots+vu^{k-2}+u^{k-1})=1$.

因 $k\geqslant 2$，上式显然不成立.

2. 由于方程左边与 p 无关，故实际上是要证明 $x>1$ 时，x^4+4^x 为合数，联想到公式 $m^4+4n^4=(m^2+2n^2+2mn)(m^2+2n^2-2mn)$，这道题就不难解决了. 记 $f(x)=x^4+4^x(x\in\mathbf{Z})$.

我们只要证明，对 $x\geqslant 2$，$f(x)$ 是合数.（事实上，当 $x<0$ 时，$f(x)\notin\mathbf{Z}$，而 $x=0$ 时 $f(x)=1$ 不为素数，$x=1$ 时 $f(x)=5$.）

若 $x=2k$（$k\geqslant 1$ 为正整数），则 $f(x)=(2k)^4+4^{2k}=4^2\times[k^4+4^{2(k-1)}]$ 为合数.

若 $x=2k+1$（$k\geqslant 1$ 为正整数），则 $f(x)=(2k+1)^4+4\times 2^{4k}=[(2k+1)^2+2^{2k+1}+2^{k+1}\cdot(2k+1)][(2k+1)^2+2^{2k+1}-2^{k+1}(2k+1)]$ 为合数.

从而原命题得证.

3. 若方程 $ax+by=ab-a-b$ 有非负整数解 (x_0,y_0)，则 $a(x_0+1)+b(y_0+1)=ab$，于是 $a|b(y_0+1)$，$b|a(x_0+1)$，结合 $(a,b)=1$，可知 $a|(y_0+1)$，$b|(x_0+1)$，导致 $a(x_0+1)+b(y_0+1)\geqslant 2ab$，矛盾. 另一方面，设 $c\in\mathbf{N}^*$，$c>ab-a-b$，则由方程 $ax+by=c$ 的通解形式，可知存在解 (x_0,y_0)，使得 $0\leqslant x_0<b$，这时 $by_0=c-ax_0>ab-a-b-a(b-1)=-b$，故 $y_0>-1$，从而 $y_0\geqslant 0$. 于是，原方程有非负整数解.

综上，所求 $c_0=ab-a-b+1$.

4. 由上题知，若 $c\in\mathbf{N}^*$，使 $ax+by=c$ 无非负整数解，则 $c\in[0,ab-a-b]$. 于是，该方程的解 (x_0,y_0) 若满足 $0\leqslant x_0<b$，则 $y_0<0$，且 $ab-a-b-c=ab-a-b-ax_0-by_0=a(b-1-x_0)+b(-1-y_0)$，这表明方程 $ax+by=ab-a-b-c$ 有非负整数解 $(b-1-x_0,-1-y_0)$. 反之，若 $c\in[0,ab-a-b]$，使方程 $ax+by=c$ 有非负整数解，则方程 $ax+by=ab-a-b-c$ 无非负整数解（否则，$ax+by=ab-a-b$ 有非负整数解，与上题的结论矛盾）.

所以，所求 c 的个数为 $\frac{1}{2}(ab-a-b+1)=\frac{1}{2}(a-1)(b-1)$.

5. 显然$(a,b)=(2,1)$为原方程的解. 下设$b>1$,设$(a,b)=d$,则

$a=a_1d,b=b_1d$,这里$(a_1,b_1)=1$,于是原方程可写成

$a_1[a_1b_1^2d^2+a_1(da_1-1)-3b_1]=b_1^2(db_1+1)$.

因b_1整除上式右边,故也整除左边,从而$b_1\mid(db_1-1)$,即$b_1\mid(a-1)$. 因$a>1$,故$a_1\geqslant b_1$. 注意到$b>1$,有$(a+b)^2>(a^2-b)(a+b)\Rightarrow a+b>a^2-b$,即$2b>a(a-1)$,所以$2>\frac{a(a-1)}{b}=a_1\cdot\frac{a-1}{b_1}\geqslant a_1$.

故$a_1=1$,且$a-1=b_1$,从而$b=b_1d=a(a-1)$,代入原方程,得$a+a^2(a-1)^2=a^3$.

上式左边应被a^2整除,即$a^2\mid a$,从而$a=1$,这不可能. 因此方程仅有正整数解$(a,b)=(2,1)$.

6. 注意到,当$y>0$或$y<-3$时,均有$y^3<y^3+2y+1<(y+1)^3$,这时y^3+2y^2+1不是立方数,原方程无解. 于是,只要考虑$y=-3,-2,-1,0$的情形,分别代入,得方程的整数解为$(x,y)=(-2,-3),(1,-2)$或$(1,0)$.

7. 由条件知,a,b,c为奇数,若d为奇数,则$a^2-b^2+c^2-d^2$为偶,矛盾. 故d为偶数,从而$d=2$,进而$a^2-b^2+c^2=1753$. 由条件,又可知$a\geqslant 3b+2,b\geqslant 2c+1,c\geqslant 5$.

故 $1753\geqslant(3b+2)^2-b^2+c^2=8b^2+12b+4-c^2\geqslant 8(2c+1)^2+12b+4$

$=33c^2+32c+12b+12\geqslant 33c^2+160+132+12$,

所以$c^2<40$,故$c\leqslant 6$,结合$c\geqslant 5$及c为素数,可知$c=5$,这样有$(a-b)(a+b)=1728=2^6\times 3^3$,结合$a>3b$,知$a-b>2b\geqslant 22$,及$a-b$与$a+b$均为偶数,且$a,b$都是奇数,可得$a-b=32,a+b=54$,故$a=43,b=11$,进而$a^2+b^2+c^2+d^2=1999$.

8. 设(x,y)为方程的整数解,则$3\mid x^2$. 设$x=3x_1$,则$3x_1^2+y^2=1998x$,从而,$3\mid y^2$. 设$y=3y_1$,则$x_1^2+3y_1^2=666x_1$. 由此类推,可设$x=27m,y=27n$,得

$m^2+3n^2=74m\Rightarrow(m-37)^2+3n^2=37^2$.

对上式作奇、偶性分析,可知m,n均为偶数,于是$3n^2\equiv 37^2-(m-37)^2\equiv 0\pmod 8$,故$4\mid n$,设$n=4r$,则$48r^2\leqslant 37^2$,从而$r^2\leqslant 28$,故$|r|\leqslant 5$,对$|r|=0,1,\cdots,5$. 计算$37^2-48r^2$的值,可知仅当$|r|=0,5$时,$37^2-48r^2$为完全平方数,所以$(x,y)=(0,0),(1998,0),(1458,\pm 540)$或$(540,\pm 540)$.

9. 假设原方程存在整数解(x,y). 若$11\mid y$,则$x^2\equiv 7\pmod{11}$;若$11\nmid y$,则由费马小定理,可知$11\mid(y^{10}-1)$,即$11\mid(y^5-1)(y^5+1)$. 由于$(y^5-1,y^5+1)\mid x$,故$y^5\equiv\pm 1\pmod{11}$,故$x^2\equiv 6$或$8\pmod{11}$. 所以,要求$x^2\equiv 6,7$或$8\pmod{11}$,但是,对$x\equiv 0,\pm 1,\pm 2,\pm 3,\pm 4,\pm 5\pmod{11}$讨论,可知$x^2\equiv 0,1,4,9,5$或$3\pmod{11}$,不会出现$x^2\equiv 6,7$或$8\pmod{11}$的情形. 矛盾.

10. 注意到$(x,y,z,u,v)=(1,2,3,4,5)$是原方程的正整数解.

一般地,设(x,y,z,u,v)是原方程的正整数解,且$x<y<z<u<v$,则将原方程视为关于x的一元二次方程,可知$(yzuv-x,y,z,u,v)$也是原方程的正整数解. 依对称性,可知$(y,z,u,v,yzuv-x)$也是解,且满足$y<z<u<v<yzuv-x$. 依此递推方式,可得原方程的无穷多组正整数解,并且后一解中,最小的数比前一组解中最小的数严格地大. 所以,存在满足要求的正整数解.

11. 我们分$p=q$和$p\neq q$两种情况来解,记原方程为(*).

(1) $p=q$时,(*)式化为:$2p(p+1)=r(r+1)$. ①

明显地,r是奇素数,从而由①可知$2p\mid r+1$,故$2p\leqslant r+1$. 再利用①便有$r(r+1)=2p(p+1)\leqslant(r+1)(p+1)$,于是$r\leqslant p+1$,故$2p\leqslant r+1\leqslant p+1+1=p+2$,也即$p\leqslant 2$,从而只有$p=2$,此时$r=3$.

(2) $p\neq q$ 时,注意到 $p(p+1)+q(q+1)\leqslant(p+q-1)(p+q)$,于是,利用(*)便有

$r\leqslant p+q-1$. ②

将(*)式移项、因式分解得 $p(p+1)=(r-q)(r+q+1)$. ③

注意到②,由③我们便可得到 $p\mid r+q+1$,同理可得 $q\mid r+p+1$. 注意到 p、q 是不同的素数,那么,由 $p\mid r+p+q+1$,$q\mid r+p+q+1$ 可知

$pq\mid(r+p+q+1)$.

于是 $pq\leqslant r+p+q+1\leqslant 2(p+q)$,也即是

$(p-2)(q-2)\leqslant 4$. ④

设 $p>q$,穷举可知满足④的 (p,q) 只有 $(5,3)$,和 $q=2$,p 是任意奇素数. 若 $(p,q)=15,37$,此时 $r(r+1)=36$,这不可能;若 $q=2$,由 $2\mid(r+p+1)$ 即知 r 是偶数,这也不可能,故 $p\neq q$ 时无解.

满足(*)的素数 (p,q,r) 为 $(2,2,3)$.

这时我们反复利用了一个重要的技巧:如果正整数 a、b 满足 $a\mid b$,那么 $a\leqslant b$.

12. 由 $y^2=(x-1)(x^6+x^5+\cdots+1)$ 及 $(x-1,x^6+x^5+\cdots+1)=(x-1,7)=1$ 或 7,可知若 $7\nmid y$,那么就有整数 z,使得 $x^6+x^5+\cdots+1=z^2$,明显地 x 是奇数,且在 $x>6$ 时 $\left(4x^3+2x^2+\frac{3}{2}x+\frac{1}{2}\right)^2<16(x^6+x^5+\cdots+1)=(4z)^2<\left(4x^3+2x^2+\frac{3}{2}x+\frac{3}{2}\right)^2$,即 $4z$ 位于两个相邻整数之间,故它不是整数,那么只有 $x=1,3,5$,但此时 z 亦不是整数,得到了矛盾,从而 $7\mid y$.

13. 我们比较方程 $n!=a!\,b!$ 中左、右两式中因子 2 的个数可以得到

$$\sum_{j=1}^{\infty}\left[\frac{a}{2^j}\right]+\sum_{j=1}^{\infty}\left[\frac{b}{2^j}\right]=\sum_{j=1}^{\infty}\left[\frac{n}{2^j}\right]. \qquad (*)$$

设 $2^k\leqslant n<2^{k+1}$,从而 $a,b\leqslant n<2^{k+1}$. 对(*)式应用不等式 $[x]>x-1$ 及 $[x]\leqslant x$,便知:

$$\sum_{j=1}^{k}\left(\frac{a}{2^j}-1\right)+\sum_{j=1}^{k}\left(\frac{b}{2^j}-1\right)<\sum_{j=1}^{\infty}\left[\frac{a}{2^j}\right]+\sum_{j=1}^{\infty}\left[\frac{b}{2^j}\right]=\sum_{j=1}^{\infty}\left[\frac{n}{2^j}\right]\leqslant\sum_{j=1}^{\infty}\frac{n}{2^j}=n,$$

也即 $\left(1-\frac{1}{2^k}\right)(a+b)<n+2k$,

从而 $a+b<n+2k+\frac{1}{2^k}(a+b)\leqslant n+2k+\frac{2n}{2^k}\leqslant n+2\log_2 n+4$.

于是原题得证.

14. 设 (λ,μ) 是方程 $x^2-pqy^2=1$(*)的一组正整数解,于是

$$\begin{aligned}p(\lambda x^*+\mu qy^*)^2-q(\mu px^*+\lambda y^*)^2&=(x^*)^2(p\lambda^2-q\mu^2p^2)-(y^*)^2(q\lambda^2-p\mu^2q^2)\\&=[p(x^*)^2-q(y^*)^2](\lambda-pq\mu^2)=1.\end{aligned}$$

可见,$(\lambda x^*+\mu qy^*,\mu px^*+\lambda y^*)$ 也是方程(*)的一组正整数解,重复上述过程,便可构造出(*)的无穷多组正整数解.

这种构造性的解法来源于寻求参数 $\alpha,\beta,\gamma,\delta$,使 $(\alpha x^*+\beta y^*,\gamma x^*+\delta y^*)$ 也满足(*). 此时 $\alpha,\beta,\gamma,\delta$ 满足 $p\alpha^2-q\gamma^2=p$,$p\beta^2-q\delta^2=-q$,$p\alpha\beta=q\gamma\delta$.

令 $\gamma=pk$,$\beta=qs$,上述条件组化成 $\alpha^2-pqk^2=1$,$\delta^2=pqs^2=1$,$\alpha s=k\delta$.

从而只要取 $\alpha=\delta$,$k=s$ 即可.

15. 设 $x^2+y^2\quad x\quad k\cdot 2xy(k\in\mathbf{N})$. 将上式化成关于 y 的一元二次方程

$y^2-2kxy+x^2-x=0$.

因为它是整系数的且根为整数，故其判别式

$\Delta=(2kx)^2-4(x^2-x)=4x(kx^2-x-1)$是完全平方数，也即$x(kx^2-x-1)$是完全平方数，但是注意到$(x,kx^2-x-1)=1$，于是$x$是完全平方数，证毕.

16. 由条件可知

$(n-k)^2-(m-l)^2=(n+k)^2-(m+l)^2=(n+k+m+l)(n+k-m-l)$.

又依题意可知$n-k>m-l$，所以$n+k>m+l$.

从而$n+k-m-l\geqslant1$，以及

$$n+k+m+l=n+k-m-l+2(m+l)\geqslant1+2(k+1+k+2)=4k+7. \quad ①$$

于是由①，我们便知道：$(n-k)^2\geqslant(m-l)^2+4k+7\geqslant1+4k+7=4k+8$，

从而$\left(\frac{n-k}{2}\right)^2\geqslant k+2$，原题得证.

注 从证明过程可知，等号仅在$k=2,l=3,m=4,n=6$时取得.

17. 由$5^z\cdot7^w+1$为偶数，知$x\geqslant1$.

情形Ⅰ：若$y=0$，此时$2^x-5^z\cdot7^w=1$.

若$z\neq0$，则$2^x\equiv1\pmod 5$，由此得$4|x$. 因此$3|(2^x-1)$，这与$2^x-5^z\cdot7^w=1$矛盾.

若$z=0$，则$2^x-7^w=1$.

当$x=1,2,3$时，直接计算可得$(x,w)=(1,0),(3,1)$.

当$x\geqslant4$时，有$7^w\equiv1\pmod{16}$，直接计算知这不可能.

所以，当$y=0$时，全部的非负整数解为$(1,0,0,0),(3,0,0,1)$.

情形Ⅱ：若$y>0,x=1$，则$2\cdot3^y-5^z\cdot7^w=1$.

因此$-5^z\cdot7^w\equiv1\pmod 3$，即$(-1)^z\equiv-1\pmod 3$，从而$z$为奇数，故$2\cdot3^y\equiv1\pmod 5$，由此知$y\equiv1\pmod 4$.

当$w\neq0$时，有$2\cdot3^y\equiv1\pmod 7$，因此得$y\equiv4\pmod 6$. 此与$y\equiv1\pmod 4$矛盾，所以$w=0$. 于是$2\cdot3^y-5^z=1$.

当$y=1$时，$z=1$；当$y\geqslant2$时，有$5^z\equiv-1\pmod 9$，由此知$z\equiv3\pmod 3$，因此$(5^3+1)|(5^z+1)$，故$7|(5^z+1)$，这与$5^z+1=2\cdot3^y$矛盾. 故此种情形的解为$(1,1,1,0)$.

情形Ⅲ：若$y>0,x\geqslant2$，分别将原方程模4及模3，得到$5^z\cdot7^w\equiv-1\pmod 4$，$5^z\cdot7^w\equiv-1\pmod 3$，即$(-1)^w\equiv-1\pmod 4$，$(-1)^z\equiv-1\pmod 3$，因此$z$和$w$都是奇数，从而$2^x\cdot3^y=5^z\cdot7^w+1\equiv35+1\equiv4\pmod 8$，所以$x=2$. 原方程变为$4\cdot3^y-5^z\cdot7^w=1$（其中$z$和$w$均为奇数），由此知$4\cdot3^y\equiv1\pmod 5$，$4\cdot3^y\equiv1\pmod 7$.

从上面两式得$y\equiv z\pmod{12}$. 设$y=12m+2,m\geqslant0$，于是，

$5^z\cdot7^w=4\cdot3^y-1=(2\cdot3^{6m+1}-1)(2\cdot3^{6m+1}+1)$.

因为$2\cdot3^{6m+1}+1\equiv6\cdot2^{3m}+1\equiv6+1\equiv0\pmod 7$，

又因为$(2\cdot3^{6m+1}-1,2\cdot3^{6m+1}+1)=1$，所以$5|(2\cdot3^{6m+1}-1)$，于是

$2\cdot3^{6m+1}-1=5^z$，$2\cdot3^{6m+1}+1=7^w$.

若$m\geqslant1$，则由上式得$5^z\equiv-1\pmod 9$，这在情形Ⅱ中已证不可能.

若 $m=0$，则 $y=2,z=1,w=1$. 此种情形解为(2,2,1,1).

综上所述，所有非负整数解为(1,0,0,0)，(3,0,0,1)，(1,1,1,0)，(2,2,1,1).

习题 B

1. 解法 1　P 能取到的所有值是$\{k|k=0$ 或 $k\geqslant 2,k\in\mathbf{Z}\}$.

一方面，P 能取到下述一些值：

令 $x=2,y=8$，显然 $x<y$，且 $P=0$.

对于 $k\geqslant 2,k\in\mathbf{Z}$，令 $x=k^3,y=k^5-k$，则 $y-x=k^5-k^3-k=k^3(k^2-1)-k>0$，且 $P=\frac{k^9-(k^5-k)}{1+k^3(k^5-k)}=\frac{k^9-k^5+k}{k^8-k^4+1}=k$.

另一方面，将证 P 无法取到其他整数值.

若 $P<0$，则 $y>x^3$，从而 $0<|x^3-y|=y-x^3<y<1+xy=|1+xy|$，

即 P 的分子绝对值小于分母绝对值，从而 $P\notin\mathbf{Z}$，矛盾.

若 $P=1$，则 $x^3-y=1+xy\Rightarrow x^3-1=y(x+1)\Rightarrow(x+1)(x^2-x+1)-2=y(x+1)$，所以，$x+1|2$，从而 $x=1$，代入得 $y=0$，与题设 x,y 为正整数矛盾.

故 $P<0$ 与 $P=1$ 均不可能.

解法 2　易验证 $y=8,x=2$ 时，$P=0$.

$P=1$ 时，$x^3-y=1+xy\Rightarrow(x+1)y=x^3-1=(x+1)(x^2-x+1)-2$，所以$(x+1)|2$，$x=1$，从而 $y=0<x\Rightarrow$矛盾. 因此 $P\neq 1$.

当 $P\geqslant 2$ 时，由 $P=\frac{x^3-y}{1+xy}$可得 $y=\frac{x^3-P}{xP+1}$.

由此知，当 $x=P^3$ 时，$y=P(P^4-1)>P^3$ 成立，这说明 P 可取$\geqslant 2$ 的任意整数.

当 $P<0$ 时，由 $|x^3-y|=y-x^3<xy+1\Rightarrow$矛盾.

所以 P 可取的值为$\{k|k\in\mathbf{N},k=0$ 或 $k\geqslant 2\}$.

注　此题源于讨论方程 $x^2+y^2=z(1+xy)$ 的正整数解这一问题. 1991 年 IMO 中有一试题：设 $(xy+1)|(x^2+y^2)$，$x,y\in\mathbf{N}^*$，求证：$\frac{x^2+y^2}{1+xy}$是一个完全平方数.

探究这个问题，可以发现，如果$\frac{x^2+y^2}{1+xy}$是整数，则一定有$\frac{x^2+y^2}{1+xy}=(x,y)^2$，其中$(x,y)$表示 x,y 的最大公因数.

2. (1) 若 $m,n,r\geqslant 2$，由 $mn\geqslant 2m,nr\geqslant 2n,mr\geqslant 2r$，得

$mn+nr+mr\geqslant 2(m+n+r)$.

所以以上不等式均取等号，故 $m=n=r=2$.

若 $1\in\{m,n,r\}$，不妨设 $m=1$，则 $nr+n+r=2(1+n+r)$，于是$(n-1)(r-1)=3$，所以$\{n-1,r-1\}=\{1,3\}$，故$\{n,r\}=\{2,4\}$，$\{m,n,r\}=\{1,2,4\}$，这样的解有 3! =6 组.

所以，不定方程 $mn+nr+mr=2(m+n+r)$共有 7 组正整数解.

(2) 将 $mn+nr+mr=k(m+n+r)$化为

$[n-(k-m)][r-(k-m)]=k^2-km+m^2$.

$n=k-m+1, r=k^2-km+m^2+k-m$ 满足上式，且 $m=1,2,\cdots,\left[\frac{k}{2}\right]$时，$0<m<n<r$.

k 为偶数时，

$\{m,n,r\}=\{l,k-l+1,k^2-kl+l^2+k-l\}$，

其中 $l=1,2,\cdots,\frac{k}{2}$ 给出了不定方程的 $3k$ 组正整数解.

k 为奇数时，

$\{m,n,r\}=\{l,k-l+1,k^2-kl+l^2+k-l\}$，

其中 $l=1,2,\cdots,\frac{k-1}{2}$ 给出了不定方程的 $3(k-1)$ 组正整数解，m,n,r 中有两个 $\frac{k+1}{2}$，另一个为

$$k^2-k\frac{k+1}{2}+\left(\frac{k+1}{2}\right)^2+k-\frac{k+1}{2}=\frac{(k+1)(3k-1)}{4}$$

的情况给出了不定方程的 3 组正整数解.

而 $m=n=r=k$ 亦为不定方程的正整数解.

故不定方程 $mn+nr+mr=k(m+n+r)$ 至少有 $3k+1$ 组正整数解.

3. 因为 $x\neq 0$，显然有 $y\neq 0$.

不失一般性，假定 x,y 是题设方程的整数解，且满足 $x>0,y>0$，及 $(x,y)=1$，我们还可以进一步假定 x 是满足上述条件的最小的整数解.

由于 $z^2\equiv 0,1,4 \pmod 8$，可知 x 是偶数，而 y 是奇数. 注意到 $x^4+(x^2+y^2)^2=z^2$，及 $(x^2,x^2+y^2)=1$，故存在一个奇整数 p 和偶整数 q，使得

$x^2=2pq, x^2+y^2=p^2-q^2$ 及 $(p,q)=1$.

由此易证，存在一个整数 a 与奇数 b，使得

$p=b^2, q=2a^2$.

故 $x=2ab, y^2=b^4-4a^4-4a^2b^2$.

注意到 $\left(\frac{2a^2+b^2+y}{2}\right)^2+\left(\frac{2a^2+b^2-y}{2}\right)^2=b^4$ 及 $\left(\frac{2a^2+b^2+y}{2},\frac{2a^2+b^2-y}{2}\right)=1$.

故存在整数 s,t，其中 $s>t$，$(s,t)=1$，使得

$\frac{2a^2+b^2+y}{2}=2st, \frac{2a^2+b^2-y}{2}=s^2-t^2$，

或 $\frac{2a^2+b^2+y}{2}=s^2-t^2, \frac{2a^2+b^2-y}{2}=2st$，

及 $b^2=s^2+t^2$.

易知 $a^2=(s-t)t$.

由于 $(a,b)=1$，$(s,t)=1$，故存在正整数 $m,n((m,n)=1)$，使得

$(s-t)=m^2, t=n^2$.

因此，$b^2=n^4+(n^2+m^2)^2$.

而 $x=2ab>t=n^2\geqslant n$，这与 x 是最小解的假定矛盾.

4. $(x+y+z)[(x-y)^2+(y-z)^2+(z-x)^2]=4006$.

因为 $4006=2\times2003$，且 $(x-y)^2+(y-z)^2+(z-x)^2\equiv0\pmod 2$，

所以，$\begin{cases}x+y+z=1,\\(x-y)^2+(y-z)^2+(z-x)^2=4006,\end{cases}$ ①

或 $\begin{cases}x+y+z=2003,\\(x-y)^2+(y-z)^2+(z-x)^2=2.\end{cases}$ ②

对于①有

$(x-y)^2+(x+2y-1)^2+(2x+y-1)^2=4006$，

即 $6x^2+6y^2+6xy-6x-6y+2=4006$.

但 $4006\equiv4\pmod 6$，矛盾.

对于②，因为 $|x-y|,|y-z|,|z-x|$ 中有两个 1，一个 0，不妨设 $x\geqslant y\geqslant z$.

当 $x-1=y=z$ 时，$3y+1=2003$，无解.

当 $x=y=z+1$ 时，$3x-1=2003$，$x=668$.

因此，满足条件的三元整数组为

$(668,668,667)$，$(668,667,668)$，$(667,668,668)$.

5. 若 $p=2$，代入等式得

$q^2+r^2=4$.

这个等式没有素数解，故 p 是奇素数.

考虑 $q^2+r^2\equiv0\pmod p$，有

$p|q$，$p|r$ 或 $p=4k+1$.

在第一种情况中，因为 q,r 是素数，可以得到 $p=q=r$，这时，等式可化简为 $p^3=3p^2$.

解得 $p=q=r=3$.

在第二种情况中，

$q^2+r^2\equiv0\pmod 4$.

所以，$2|q,r$，由于 q,r 是素数，所以，$q=r=2$.

但 $p^3-p^2=8$ 无素数解，最后得到解为 $p=q=r=3$.

6. 设 $n=mk$，$k\in\mathbf{N}_+$，则

$m(7+3k)=2^{2004}\times5^{2004}$.

令 $7+3k=2^u\times5^v$，$u,v\in\mathbf{N}$.

因为上式两边模 3 同余，所以，u,v 奇偶性相同，故 k 可取 1003^2+1002^2-2 个值（不包括 $(u,v)=(0,0)$ 或 $(2,0)$）.

所以，$(m,n)=\left(\dfrac{10^{2004}}{7+3k},mk\right)$，有 $1003^2+1002^2-2=2010011$ 个解.

7. 若 $x=y$，则显然无解.

由已知方程可得

$x^y\equiv-19\pmod y$.

由于 x,y 均为素数，且 $x\neq y$，所以，$(x,y)=1$.

由费马小定理，有

$x^{y-1}\equiv 1(\bmod y)$.

于是，有 $x+19\equiv 0(\bmod y)$.

同理，$19-y\equiv 0(\bmod x)$.

因为 $x-y+19\equiv 0(\bmod y)$，$x-y+19\equiv 0(\bmod x)$，所以，

$x-y+19\equiv 0(\bmod xy)$.

易知 $x-y+19\neq 0$，于是，有

$x+y+19>|x-y+19|\geqslant xy$.

即得 $(x-1)(y-1)<20$.

因此，$|x-y|<19$，$x-y+19\geqslant xy$，即

$(x+1)(y-1)\leqslant 18$.

所以，当 $x\geqslant 5$ 时，$y=2$ 或 $y=3$.

但是 $x^2-2^x<0$，$x^3-3^x<0$，$xy^2-19>0$，矛盾.

从而，$x\leqslant 4$.

容易验证，原不定方程的解为(2,3)和(2,7).

8. 不妨设 $x\leqslant y$.

若 $2x<y+1$，则

$(2^y)^2<1+4^x+4^y<(1+2^y)^2$.

这表明，$1+4^x+4^y$ 不是完全平方数.

若 $2x=y+1$，则

$1+4^x+4^y=1+2^{y+1}+4^y=(1+2^y)^2$.

故 $(x,y,z)=(n,2n-1,1+2^{2n-1})(n\in \mathbf{N}_+)$ 就是满足条件的三元正整数组.

若 $2x>y+1$，注意到

$4^x+4^y=4^x(1+4^{y-x})=(z-1)(z+1)$.

由 $\gcd(z-1,z+1)=2$，知 $z-1$ 或 $z+1$ 能被 2^{2x-1} 整除，而对任意的正整数 $x>1$，$2(1+4^{y-x})\leqslant 2(1+4^{x-2})<2^{2x-1}-2$，矛盾.

因此，所求的所有满足条件的三元正整数组为

$(x,y,z)=(n,2n-1,1+2^{2n-1})$ 或 $(2n-1,n,1+2^{2n-1})(n\in \mathbf{N}_+)$.

9. 由观察易知 $y>x$，即 $y-x>0$.

原方程等价于

$11^3=y^3-x^3=(y-x)(y^2+xy+x^2)$.

由于 11 为素数，故 $y-x$ 只能为 $1,11,11^2$ 或 11^3.

若 $y-x=1$，则

$x^2+xy+y^2=11^3=3x^2+3x+1$.

此方程无整数解.

若 $y-x=11$，则

$11^2=x^2+xy+y^2=3x^2+3\times 11x+11^2$.

解得 $x=0,y=11$ 或 $x=-11,y=0$.

若 $y-x=11^2$,则

$11=x^2+xy+y^2=3x^2+3\times11^2x+11^4$.

因上式左边被 11 整除,故 $3x^2$ 必须能被 11 整除,所以,必须有 $11|x$. 令 $x=11z$(z 为整数),则

$1=3\times11z^2+3\times11^2z+11^3$.

上式右边能被 11 整除,而左边不能,矛盾. 故此时方程无整数解.

若 $y-x=11^3$,则

$1=x^2+xy+y^2=3x^2+3\times11^3x+11^6$.

此时,$\Delta<0$,方程无解.

综上,方程的所有解为

$$\begin{cases}x=0,\\y=11\end{cases}\text{及}\begin{cases}x=-11,\\y=0.\end{cases}$$

10. 如果 p 是 $n+1$ 的素因子,则 p 也是 $n!+1$ 的素因子. 因为 $n!+1$ 不能被任何素数 $q(q\leqslant n)$整除,所以,只能是 $p=n+1$.

如果 $n+1=2$,$n=1$ 且 $2^k-1=1$,则 $k=1$. 因此,数对(1,1)是一个解.

如果 $n+1=3$,同理,得 $3^k-1=2$ 和 $k=1$. 因此,数对(2,1)是一个解.

如果 $n+1=5$,同理,得 $5^k-1=24$ 和 $k=2$. 因此,数对(4,2)是一个解.

下面证明再没有其他的解.

假设(n,k)是满足条件的一个解,$n+1$ 是一个大于等于 7 的奇素数,那么,

$n=2m,m>2$.

因为 $2\leqslant n-1,m\leqslant n-1,n=2m$ 是$(n-1)!$ 的因子,所以 $n!$ 能被 n^2 整除. 因此,

$(n+1)^k-1=n^k+kn^{k-1}+\cdots+\frac{k(k-1)}{2}n^2+nk$ 能被 n^2 整除.

于是,k 能被 n 整除,且 $k\geqslant n$,从而,

$n!=(n+1)^k-1>n^k\geqslant n^n>n!$. 矛盾.

11. 将方程改写为

$$3^x-1=2^xy. \quad ①$$

这表明,如果(x,y)是解,则 x 不能超过 3^x-1 的标准分解中因子 2 的指数. 记 $x=2^m(2n+1)$,其中 m,n 是非负整数,于是,可得

$$3^x-1=3^{2^m(2n+1)}-1=(3^{2n+1})^{2^m}-1=(3^{2n+1}-1)\prod_{k=0}^{m-1}[(3^{2n+1})^{2^k}+1]. \quad ②$$

由于 $3^{2n+1}=(1+2)^{2n+1}\equiv[1+2(2n+1)+4n(2n+1)](\bmod 8)\equiv3(\bmod 8)$,则

$$(3^{2n+1})^{2^k}\equiv\begin{cases}3(\bmod 8),\text{当 }k=0\text{ 时};\\1(\bmod 8),\text{当}=1,2,\cdots\text{时}.\end{cases}$$

因此,对于所求的指数,当 $m=0$ 时是 1,当 $m=1,2,\cdots$时是 $m+2$. 由此可以断定,x 不能超过$m+2$.

[由上面的分析可知,式②右端可表为

$(8t+2)(8t+4)(8r_1+2)(8r_2+2)\cdot\cdots\cdot(8r_{m-1}+2)$

$=2^{m+2}(4t+1)(2t+1)(4r_1+1)(4r_2+1)\cdot\cdots\cdot(4r_{m-1}+1)$

$=2^x y$(参看式①)——译注]

故 $2^m \leqslant 2^m(2n+1)=x \leqslant m+2$.

于是，$m\in\{0,1,2\}$ 且 $n=0$.

由此可以断定，所给方程的正整数解是

$(x,y)=(1,1),(2,2),(4,5)$.

12. 原方程等价于

$(2y+x)^2=4x^3-27x^2+44x-12=(x-2)(4x^2-19x+6)=(x-2)[(x-2)(4x-11)-16]$.

当 $x=2$ 时，$y=-1$ 满足原方程.

若 $x\neq 2$，由于 $(2y+x)^2$ 是完全平方数，令 $x-2=ks^2$，其中 $k\in\{-2,-1,1,2\}$，s 为正整数. 实际上，若存在素数 p 和非负整数 m，使得 p^{2m+1} 整除 $x-2$，p^{2m+2} 不能整除 $x-2$，于是，p 能整除 $(x-2)\cdot(4x-11)-16$，则有 $p|16$，即 $p=2$.

若 $k=\pm 2$，则 $4x^2-19x+6=\pm 2n^2$，其中 n 为正整数，即

$(8x-19)^2-265=\pm 32n^2$.

由于 $\pm 32n^2\equiv 0,\pm 2 \pmod 5$，

$(8x-19)^2\equiv 0,\pm 1 \pmod 5)$，

且 $25\nmid 265$，矛盾.

若 $k=1$，则 $4x^2-19x+6=n^2$，其中 n 为正整数，

即 $265=(8x-19)^2-16n^2=(8x-19-4n)(8x-19+4n)$.

分别对

$265=1\times 265=5\times 53=(-265)\times(-1)=(-53)\times(-5)$

四种情况讨论得到相应的 x，n，使得 $x-2=s^2$ 是完全平方数.

只有 $x=6$ 满足条件，于是 $y=3$ 或 $y=-9$.

若 $k=-1$，则 $4x^2-19x+6=-n^2$，其中 n 为正整数，即

$265=(8x-19)^2+16n^2$.

由 $16n^2\leqslant 265$，得 $n\leqslant 4$.

当 $n=1$，2 时，$4x^2-19x+6=-n^2$ 无整数解；

当 $n=3$ 时，得整数解 $x=1$，于是，$y=1$ 或 -2；

当 $n=4$ 时，得整数解 $x=2$，矛盾.

综上所述，满足条件的 (x,y) 为

$\{(6,3),(6,-9),(1,1),(1,-2),(2,-1)\}$.

13. 不失一般性，设 $k\geqslant l$，则

$k!=\frac{k!}{l!}+1+\frac{m!}{l!}$.

因为方程中三项为整数，所以，最后一项必为整数，即 $m\geqslant l$.

又方程右边三项的和至少为 3，则 $k\geqslant 3$. 所以，$k!$ 为偶数.

因此，$\frac{k!}{l!}$，$\frac{m!}{l!}$ 中恰有一个为奇数.

分两种情况讨论：

(1) $\frac{k!}{l!}$为奇数，$\frac{m!}{l!}$为偶数，于是，$k\quad l+1$ 且 l 为偶数，或 $k\quad l$. 同时，有 $m\geqslant l+1$.

(i) $k=l$，于是，有 $k!=2+\frac{m!}{k!}$.

若 $k=3$，则方程的解为 $k=l=3$，$m=4$.

若 $k>3$，则 $k!$ 能被 3 整除，$k!-2$ 不能被 3 整除.

因此，$m=k+1$ 或 $m=k+2$.

于是，$\frac{m!}{k!}=k+1$ 或 $\frac{m!}{k!}=(k+1)(k+2)$，即

$k!=k+3$ 或 $k!=2+(k+1)(k+2)$.

将 $k=4$ 和 $k=5$ 代入，知均不是方程的解.

对于较大的 k 的值，方程的左边大于右边.

(ii) $k=l+1$，l 为偶数，于是，

$(l+1)!=l+2+\frac{m!}{l!}$.

由于 $(l+1)!$ 和$\frac{m!}{l!}$均能被 $l+1$ 整除，所以，$l+2$ 一定能被 $l+1$ 整除，但这是不可能的.

(2) $\frac{k!}{l!}$为偶数，$\frac{m!}{l!}$为奇数，于是，$m=l+1$ 且 l 为偶数，或 $m=l$. 同时，有 $k\geqslant l+1$.

(i) 若 $m=l$，则方程简化为 $k!\ l!=k!+2l!$，即

$\frac{k!}{l!}(l!-1)=2$.

由$\frac{k!}{l!}$为偶数，得 $l!-1=1$.

所以，$l=2$，$k!=4$，但这是不可能的.

(ii) 若 $m=l+1$，l 为偶数，则方程简化为

$k!\ l!=k!+(l+2)l!$，即 $k!(l!-1)=(l+2)l!$.

因为 $l!$ 与 $l!-1$ 互素，则 $l+2$ 必须被 $l!-1$ 整除. 只有当 $l=2$，$k!=8$ 时有可能成立，但这是不可能的.

综上所述，方程有唯一的解 $k=l=3$，$m=4$.

14. 注意到

$(a^2+b)(a+b^2)=(a+b)^4$

$\Leftrightarrow a^4+a^3b^3+ab+b^4=a^4+4a^3b+6a^2b^2+4ab^3+b^4$

$\Leftrightarrow a^3b^3+2a^2b^2+ab=4a^3b+8a^2b^2+4ab^3$

$\Leftrightarrow ab(ab+1)^2=4ab(a+b)^2$

$\Leftrightarrow ab[(ab+1)^2-4(a+b)^2]=0$

成立. 因此，$(a, 0)$ 和 $(0, b)$ 是给定方程的解，a，$b\in\mathbb{Z}$.

另外的解必须使得$(ab+1)^2-4(a+b)^2=0$ 成立.

因为$(ab+1)^2-4(a+b)^2=0$，即

$ab+1=\pm 2(a+b)$.

分两种情形讨论.

如果$ab+1=2(a+b)$，则有

$(a-2)(b-2)=3$.

于是，有

$\begin{cases}a-2=3,\\b-2=1\end{cases}$或$\begin{cases}a-2=1,\\b-2=3\end{cases}$或$\begin{cases}a-2=-3,\\b-2=-1\end{cases}$或$\begin{cases}a-2=-1,\\b-2=-3.\end{cases}$

分别解得

$a=5$，$b=3$；$a=3$，$b=5$；$a=-1$，$b=1$；$a=1$，$b=-1$.

如果$ab+1=-2(a+b)$，则有

$(a+2)(b+2)=3$.

类似地，解得

$a=1$，$b=-1$；$a=-1$，$b=1$；$a=-5$，$b=-3$；$a=-3$，$b=-5$.

综上所述，给定方程所有可能解的集合为

$\{(a,0)|a\in\mathbf{Z}\}\cup\{(0,b)|b\in\mathbf{Z}\}\cup\{(-5,-3),(-3,-5),(-1,1),(1,-1),(3,5),(5,3)\}$.

15. 存在.

如果$a=b=c=1$，则$m=12$. 令

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}-\frac{12}{a+b+c}=\frac{p(a,b,c)}{abc(a+b+c)},$$

其中$p(a,b,c)=a^2(b+c)+b^2(c+a)+c^2(a+b)+a+b+c-9abc$.

假设(x,a,b)是满足$p(x,a,b)=0$的一组解，且$x\leqslant a\leqslant b$. 由于$p(x,a,b)=0$是关于x的二次方程，所以，$y=\frac{ab+1}{x}>b$是其另外的一个解.

设$a_0=a_1=a_2=1$，定义

$$a_{n+2}=\frac{a_na_{n+1}+1}{a_{n-1}}\ (n\geqslant 1).$$

我们证明下面的结论：

(1) $a_{n-1}|(a_na_{n+1}+1)$；

(2) $a_n|(a_{n-1}+a_{n+1})$；

(3) $a_{n+1}|(a_{n-1}a_n+1)$.

其中a_{n-1}，a_n，a_{n+1}均为正整数.

当$n=1$时，以上3个结论显然成立.

假设$n=k$时以上3个结论成立.

由(1)得$a_{k-1}|(a_ka_{k+1}+1)$，即a_{k-1}与a_k互素，且$a_{k-1}|[(a_ka_{k+1}+1)a_{k+1}+a_{k-1}]$；

由(2)得$a_k|(a_{k-1}+a_{k+1})$，且$a_k|(a_ka_{k+1}^2+a_{k+1}+a_{k-1})$，所以，

$a_ka_{k-1}|(a_ka_{k+1}^2+a_{k+1}+a_{k-1})$，

即 $a_k \mid \left(a_{k+1}\frac{a_ka_{k+1}+1}{a_{k-1}}+1\right)=a_{k+1}a_{k+2}+1.$

于是，当 $n=k+1$ 时，(1) 也成立.

同理，由于 a_{k-1} 与 a_{k+1} 也互素，且 $a_{k-1}\mid(a_ka_{k+1}+1+a_ka_{k-1})$，由(3)得 $a_{k+1}\mid(a_{k-1}a_k+1)$，且 $a_{k+1}\mid(a_{k-1}a_k+1+a_ka_{k+1})$. 所以，

$a_{k-1}a_{k+1}\mid[a_k(a_{k-1}+a_{k+1})+1]$，

即 $a_{k+1}\mid\left(a_k+\frac{a_ka_{k+1}+1}{a_{k-1}}\right)=a_k+a_{k+2}.$

于是，当 $n=k+1$ 时，(2) 也成立.

由 a_{k+2} 的定义及 (1) 知 a_{k+2} 是整数，且

$a_{k+2}\mid(a_ka_{k+1}+1).$

于是，当 $n=k+1$ 时，(3) 也成立.

从而可得数列 $\{a_n\}$，当 $n\geqslant2$ 时严格递增，且 $p(a_n,a_{n+1},a_{n+2})=0$，即 (a_n,a_{n+1},a_{n+2}) 是原方程的解，$\{a_n\}=\{1,1,1,2,3,7,11,26,41,97,153,\cdots\}$.

16. 原方程等价于

$(n^3-n+1)(n^2+n+1)=7^m.$

显然，$n\neq1$.

当 $n=2$ 时，$m=2$.

当 $n\geqslant3$ 时，

$n^3-n+1=n(n^2-1)+1>1$，

$n^2+n+1>1.$

设 $n^3-n+1=7^a$，$n^2+n+1=7^b$，其中，a，b 为正整数，于是，

$(n-1)(7^b-1)=7^a-1$，即 $(7^b-1)\mid(7^a-1)$.

设 $a=bq+r$，且 q 为正整数，r 为非负整数，$0\leqslant r<b$.

若 $r\neq0$，则

$7^a-1=7^{bq+r}-1=7^r(7^{bq}-1)+7^r-1.$

因为 $7^{bq}-1=(7^b-1)[7^{b(q-1)}+7^{b(q-2)}+\cdots+7^b+1]$，所以，

$(7^b-1)\mid(7^r-1)$，

矛盾. 因此，$r=0$.

设 $a=bk(k\in\mathbf{N}_+)$，则

$n^3-n+1=7^a=7^{bk}=(n^2+n+1)^k.$

当 $k=1$ 时，有

$(n^3-n+1)-(n^2+n+1)=n[n(n-1)-2]>0$，

矛盾.

当 $k\geqslant2$ 时，有

$(n^3-n+1)-(n^2+n+1)^k\leqslant(n^3-n+1)-(n^2+n+1)^2=-n^4-n^3-3n^2-3n<0$，

矛盾.

综上所述，$n=2$，$m=2$ 是原方程的唯一一组解.

17. 没有整数解.

引理　若 x 是整数，p 是 $\frac{x^7-1}{x-1}$ 的素因数，则要么 $p\equiv1(\mathrm{mod}\ 7)$，要么 $p=7$.

引理的证明：由于 $p\left|\frac{x^7-1}{x-1}\right.$，因此，$p|(x^7-1)$.

于是，$(x,p)=1$.

由费马小定理有 $x^{p-1}\equiv1(\mathrm{mod}\ p)$.

假设 $7\nmid(p-1)$，则 $(p-1,7)=1$.

由裴蜀定理，存在整数 k，m，使得

$7k+(p-1)m=1$.

则 $x\equiv x^{7k+(p-1)m}\equiv(x^7)^k(x^{p-1})^m\equiv1(\mathrm{mod}\ p)$.

故 $\frac{x^7-1}{x-1}=x^6+x^5+\cdots+1\equiv7(\mathrm{mod}\ p)$.

因此，$p\mid7$. 从而，$p=7$.

回到原题.

由引理可知，$\frac{x^7-1}{x-1}$ 的每一个正因数 d，要么 $d\equiv0\ (\mathrm{mod}\ 7)$，要么 $d\equiv1\ (\mathrm{mod}\ 7)$.

假设 x，y 是方程的一组整数解.

因为对于所有的 $x\neq1$，都有 $\frac{x^7-1}{x-1}>0$，所以，$y-1>0$.

又 $(y-1)\left|\frac{x^7-1}{x-1}=y^5-1\right.$，则

$y\equiv1\ (\mathrm{mod}\ 7)$ 或 $y\equiv2\ (\mathrm{mod}\ 7)$.

若 $y\equiv1\ (\mathrm{mod}\ 7)$，则

$y^4+y^3+y^2+y+1\equiv5\ (\mathrm{mod}\ 7)$；

若 $y\equiv2\ (\mathrm{mod}\ 7)$，则

$y^4+y^3+y^2+y+1\equiv3\ (\mathrm{mod}\ 7)$.

由于 $y^4+y^3+y^2+y+1$ 也是 $\frac{x^7-1}{x-1}$ 的因数，但其模 7 的余数不是 0 或 1，矛盾.

因此，方程没有整数解.

18. 所给问题就是求满足方程组

$$abc+d=abd+c=acd+b=bcd+a \qquad ①$$

的所有四元实数组 (a, b, c, d).

因为方程组①关于所有变量是对称的，所以，解的任何排列也是一个解. 注意到这一点，可分下列 5 种情形考虑：

(1) $a=b=c=d$；

(2) $a=b=c\neq d$；

(3) $a=b\neq c=d$；

(4) $a=b\neq c$ 且 $c\neq d$，$d\neq b$；

(5) 没有两个相等.

注意到由①的第一个方程 $abc+d=abd+c$，得

$abc-abc-c+d=0$，即 $(c-d)(ab-1)=0$.

因此，由给定方程组①还可得到类似的方程：

$(a-b)(cd-1)=0$，

$(a-c)(bd-1)=0$，

$(a-d)(bc-1)=0$，

$(b-c)(ad-1)=0$，

$(b-d)(ac-1)=0$.

下面考虑每种可能的情形.

(1) 如果 $a=b=c=d=r$，对于任何实数 r 都有解. 此时，①中 4 个表达式都等于 r^2+r，因此，解集是 $S_1=\{(r,r,r,r)|r\in\mathbf{R}\}$.

(2) 如果 $a=b=c\neq d$，由 $(c-d)(ab-1)=0$，得 $ab=1$，即 $b=\frac{1}{a}$ 一定成立.

又因为 $a=b$，于是，$a^2=1$，故 $a=\pm1$.

实际上，取 $a=b=c=\pm1$ 和 $d=r\neq a$，①中 4 个表达式都等于 $r\pm1$. 把所有的排列都考虑进去，这种情形的解集是

$S_2=\{(\pm1,\pm1,\pm1,r),(\pm1,\pm1,r,\pm1),(\pm1,r,\pm1,\pm1),(r,\pm1,\pm1,\pm1)|r\in\mathbf{R}\}$.

(3) 如果 $a=b\neq c=d$，由 $(b-c)(ad-1)=0$，得 $ad=1$，即 $d=\frac{1}{a}$.

实际上，取 $a=b=r$ 和 $c=d=\frac{1}{r}$，①中 4 个表达式都等于 $r+\frac{1}{r}$. 把所有的排列都考虑进去，这种情形的解集是

$$S_3=\left\{\left(r,r,\frac{1}{r},\frac{1}{r}\right),\left(r,\frac{1}{r},r,\frac{1}{r}\right),\left(r,\frac{1}{r},\frac{1}{r},r\right)\middle|r\in\mathbf{R},r\neq0\right\}.$$

(4) 如果 $a=b\neq c$，且 $c\neq d$，$d\neq b$，得

$1=ad=ab=ac$，即 $b=c=d$，

矛盾.

因此，这种情形没有解.

(5) 同 (4) 的理由，这种情形也没有解.

综上可知，题设方程组所有解的集合为集

$S=S_1\cup S_2\cup S_3$.

19. 因为方程 $x_1+x_2+\cdots+x_k=m$ 的非负整数解的个数为 C_{m+k-1}^{m}，而使 $x_1\geqslant1$，$x_i\geqslant0$ $(i\geqslant2)$ 的整数解个数为 C_{m+k-2}^{m-1}. 现取 $m=7$，可知，k 位"吉祥数"的个数为 $P(k)=C_{k+5}^{6}$.

2005 是形如 $\overline{2abc}$ 的数中最小的一个"吉祥数"，且 $P(1)=C_6^6=1$，$P(2)=C_7^6=7$，$P(3)=C_8^6=28$，对于四位"吉祥数" $\overline{1abc}$，其个数为满足 $a+b+c=6$ 的非负整数解个数，即 $C_{6+3-1}^{6}=28$ 个.

因为 2005 是第 $1+7+28+28+1=65$ 个"吉祥数"，即 $a_{65}=2005$，从而 $n=65$，$5n=325$.

又 $P(4)=C_9^3=84$, $P(5)=C_{10}^4=210$，而 $\sum_{k=1}^{5}P(k)=330$.

所以从大到小最后六个五位“吉祥数”依次是：70000，61000，60100，60010，60001，52000.

故第 325 个“吉祥数”是 52000，即 $a_{325}=52000$.

20. 设 $N(x^y)$ 表示整数 x^y 的个数.

若 $1<x^y\leqslant 10^6$，由于 $2^{19}=524288<10^6$，$2^{20}>10^6$，则由容斥原理得

$$N(x^y)=N(x^2)+N(x^3)+N(x^5)+N(x^7)+N(x^{11})+N(x^{13})+N(x^{17})+N(x^{19})-N(x^6)-N(x^{10})-N(x^{14})-N(x^{15}).$$

由于大于 1 且不大于 10^6 的平方数有 10^3-1 个，所以

$N(x^2)=999$.

大于 1 且不大于 10^6 的平方数有 10^2-1 个，即 $N(x^3)=99$ 个.

因为 $15^5=819375<10^6$，

所以大于 1 不大于 10^6 的 5 次方数有 $15-1$ 个，即 $N(x^5)=14$.

以此类推可得，$1<x^y\leqslant 10^6$ 时，

$N(x^y)=999+99+14+6+2+1+1-9-2-1-1=1110$ 个.

又 $n=1$ 时有非负整数解 $x>1$ 且 $y=0$.

于是满足题意的整数 n 有 1111 个.

21. **解法 1** 由于 $5-5(p+1)+(77p-1)+1=66p$，则 $x=1$ 是原三次方程的一个自然数解.

由综合除法将原三次方程降为二次方程

$$5x^2-5px+66p-1=0. \quad ①$$

本题转化为：求一切实数 p，使方程①有两个自然数解.

设 u，v $(u\leqslant v)$ 是方程①的两个自然数解，由韦达定理可以得出

$$\begin{cases} v+u=p, & ② \\ vu=\dfrac{1}{5}(66p-1). & ③ \end{cases}$$

从②，③中消去 p 得

$$5uv=66(u+v)-1. \quad ④$$

由④可知，u，v 都不能被 2，3，11 整除.

由④得 $v=\dfrac{66u-1}{5u-66}$. ⑤

因为 u，v 为自然数，则

$u>\dfrac{66}{5}$，有 $u\geqslant 14$.

又 $2\nmid u$，$3\nmid u$，则 $u\geqslant 17$.

再由 $v\geqslant u$ 得 $\dfrac{66u-1}{5u-66}\geqslant u$，即 $5u^2-132u+1\leqslant 0$.

于是有 $u\leqslant\dfrac{66+\sqrt{66^2-5}}{5}<\dfrac{132}{5}$.

故 $17\leqslant u\leqslant 26$.

再由 $2\nmid u$，$3\nmid u$，$11\nmid u$ 可知，u 只能取 17，19，23，25. 下面分别进行讨论：

当 $u=19$ 时，由⑤，$v\notin \mathbf{N}$，舍去；

当 $u=23$ 时，由⑤，$v\notin \mathbf{N}$，舍去；

当 $u=25$ 时，由⑤，$v\notin \mathbf{N}$，舍去；

当 $u=17$ 时，由⑤，$v=59$.

所以，仅当 $p=u+v=17+59=76$ 时，方程①的两根均为自然数，从而，原方程的三根均为自然数.

解法 2 由解法 1 中⑤式得

$$v=\frac{66u-1}{5u-66}=13+\frac{u+857}{5u-66}=13+\frac{1}{5}\left(1+\frac{4351}{5u-66}\right)=13+\frac{1}{5}\left(1+\frac{19\times 229}{5u-66}\right).$$

由于 v 为整数，则 $5u-66\mid 19$ 或 $5u-66\mid 229$.

由于 19，229 均为素数，则有

$5u-66=19$ 或 $5u-66=229$.

当 $5u-66=19$ 时，$u=17$，$v=59$.

当 $5u-66=229$ 时，$u=59$，$v=17$，与假设 $u\leqslant v$ 矛盾.

所以 $p=u+v=76$.

解法 3 由解法 1，方程①有自然数的必要条件是 $\Delta=25p^2-4\times 5(66p-1)$ 是完全平方数.

设 $25p^2-20(66p-1)=q^2$，则

$(5p-132)^2-17404=q^2$.

设 $5p-132=m$，则 $m^2-q^2=17404$.

从而，m 和 q 均为偶数.

设 $m=2m_0$，$q=2q_0$，则

$m_0^2-q_0^2=4351=19\times 229$.

由 $m>q$ 得 $\begin{cases}m_0-q_0=1,\ 19,\ 229,\ 4351,\\ m_0+q_0=4351,\ 229,\ 19,\ 1.\end{cases}$

解得 $m_0=\pm 2176$，± 124.

因而 $5p-132=2m_0=\pm 4352$，± 248.

由解法 1 中②式可知，p 为自然数，由③知，u，v 为奇数，再由②式知，p 为偶数.

于是可解得 $p=76$.

22. 由 $f(x)=3x+2$ 得

$f(x)+1=3(x+1)$，

从而，对于给定的 x，有

$f^{(n+1)}(x)+1=3[f^{(n)}(x)+1], n=0,1,2,\cdots$.

于是，数列 $\{f^{(n)}(x)+1\}$ 是以 3 为公比的等比数列，因而

$f^{(n)}(x)+1=3^n(x+1)$，$n=0$，1，2，$\cdots$.

这样，要证明存在正整数 m，使得 $f^{(100)}(m)$ 能被 1988 整除，等价于要证方程

$3^{100}(x+1)-1=1988y$,

即 $3^{100}(x+1)-1988y=1$ ①

有整数解,且 x 为正整数.

因为 $(3^{100},1988)=1$,所以方程①必有整数解.

设 (x_0, y_0) 是方程①的一组特解,则①的所有整数解可表示为

$$\begin{cases}x=x_0+1988t,\\ y=y_0+3^{100}t.\end{cases}$$

其中 t 为任意整数.

取足够大的 t,使由上式给出的 x,y 均为正整数.此时令 $m=x$,则 $f^{(100)}(m)$ 能被 1988 整除.

23. 假设数列中有两项之比为 p^{2l},即

$$\frac{\frac{x(x+1)}{2}}{\frac{y(y+1)}{2}}=p^{2l},x,y\in \mathbf{N},$$

则本题等价于不定方程

$x(x+1)=p^{2l}y(y+1)$

无正整数解.

设 $p^l=k$,则不定方程化为

$x^2+x=k^2y^2+k^2y$, ①

即 $(ky-x)(ky+x)=x-k^2y$.

如果 $ky-x\geqslant 0$,则必有

$x-k^2y\geqslant 0$,

从而 $(ky-x)+(x-k^2y)\geqslant 0$,

$ky(1-k)\geqslant 0$.

然而 $k>1$,$y\geqslant 1$,出现矛盾.因此必有

$ky-x<0$.

于是可令 $x=ky+a\ (a\geqslant 1)$,代入①得

$(ky+a)^2+(ky+a)=k^2y^2+k^2y$,即

$a(a+1)=ky(k-2a-1)$. ②

由于 $(a,a+1)=1$,$k=p^l$ 及 p 是素数,则由②必有

$k\mid a$ 或 $k\mid a+1$.

因此 $a\geqslant k$.

然而此时②式右边 $k-2a-1<0$,出现矛盾.

所以不定方程①无正整数解,即数列 $\left\{\frac{n(n+1)}{2}\right\}$ 中没有两项之比为 p^{2l},p 是素数.

24. (1) 当 $y=0$ 时,方程无整数解.

(2) 当 $x=0$ 时,$y=\pm 1$,因此方程有解 $x=0$,$y=1$,和 $x=0$,$y=-1$.

(3) 若 (x_0,y_0) 是方程的解,则 $(x_0,\pm y_0)$ 以及 $(-x_0,\pm y_0)$ 也是方程的解,因此只需考虑方程

的自然数解.

我们证明方程

$$2x^4+1=y^2 \quad ①$$

无自然数解.

若①有自然数解 (x, y)，则 y 是奇数. 设 $y=2z+1$，于是①化为

$$x^4=2z(z+1).$$

因此 x 为偶数，记作 $x=2u$，从而有

$$8u^4=z(z+1).$$

由$(z,z+1)=1$,可有

Ⅰ. $\begin{cases} z=8v^4, \\ z+1=w^4, \ (v, w)=1. \\ vw=u, \end{cases}$

Ⅱ. $\begin{cases} z=v^4, \\ z+1=8w^4, \ (v, w)=1. \\ vw=u, \end{cases}$

对于情形Ⅱ，有方程 $8w^4=v^4+1$. 由于

$$v^4\equiv0, 1 \pmod 8,$$

$$8w^4\equiv0 \pmod 8,$$

于是情形Ⅱ无解.

对于情形Ⅰ，有

$$w^4=8v^4+1,$$

从而 w 是奇数. 设 $w=2q+1$，则

$$(2q+1)^4=8v^4+1,$$

$$v^4=2q^4+4q^3+3q^2+q=q(q+1)(2q^2+2q+1).$$

显然 $(q,q+1,2q^2+2q+1)=1$,

所以应有 $\begin{cases} q=\alpha^4, \\ q+1=\beta^4, \end{cases}$

即 $\beta^4-\alpha^4=1.$

此方程无自然数解，于是①无自然数解.

综合 (1)，(2)，(3)，已知方程的所有整数解$(x,y)=(0,1),(0,-1)$.

25. 首先用数学归纳法证明：若 $r+s=t$ 为奇数，r，$s\in \mathbf{N}_+$，则 $ra+sb\in S$.

对 t 利用数学归纳法.

当 $t=1$ 时显然.

若 $t=2k-1$ 时结论成立，则当 $t=2k+1$ 时显然 r，s 不全小于 2，无妨设 $r\geqslant2$，由归纳假设，$(r-2)a+sb\in S$，则在 (2) 中取

$$x=(r-2)a+sb, y=z=a,$$

得 $ra+sb=x+y+z\in S,$

从而结论成立.

回到原题，由$(a,b)=1$知,对任意正整数$c>2ab$，存在

$$\begin{cases}r=r_0+bt,\\ s=s_0-at,\end{cases}(t\in\mathbf{Z})$$

使得$ra+sb=c$，分别适当取t为t_1，$t_2(=t_1+1)$使

$r_1=r_0+t_1b\in[0,b)$，$r_2=r_0+t_2b\in[b,2b)$，

于是 $s_1=\frac{c-r_1a}{b}\in\left(\frac{c-ab}{b},\frac{c}{b}\right]$，

故$s_1>a$，$s_2=\frac{c-r_2a}{b}>\frac{c-2ab}{b}>0$，

因此 $(r_1,s_1),(r_2,s_2)\in\mathbf{N}_+^2$.

由$(r_2+s_2)=(r_1+s_1)+(b-a)$知$r_1+s_1$，$r_2+s_2$恰一奇一偶. 选取使得$r_i+s_i$为奇数的那一组，利用前面的结论即知命题成立.

26. 由于任何奇平方数被4除余1，任何偶平方数是4的倍数，因2005被4除余1，故a^2，b^2，c^2三数中，必是两个偶平方数，一个奇平方数.

设$a=2m$，$b=2n$，$c=2k-1$，m，n，k为正整数，原方程化为：

$m^2+n^2+k(k-1)=501.$ ①

又因任何平方数被3除的余数，或者是0，或者是1，今讨论k：

(i) 若$3\mid k(k-1)$，则由①，$3\mid m^2+n^2$，于是m，n都是3的倍数.

设$m=3m_1$，$n=3n_1$，并且$\frac{k(k-1)}{3}$是整数，由①

$3m_1^2+3n_1^2+\frac{k(k-1)}{3}=167$， ②

于是 $\frac{k(k-1)}{3}\equiv167\equiv2\pmod 3$.

设 $\frac{k(k-1)}{3}=3r+2$，则

$k(k-1)=9r+6.$ ③

且由①，$k(k-1)<501$，所以$k\leqslant22$.

故由③，k可取3，7，12，16，21，代入②分别得到如下情况：

$\begin{cases}k=3,\\ m_1^2+n_1^2=55,\end{cases}$ $\begin{cases}k=7,\\ m_1^2+n_1^2=51,\end{cases}$ $\begin{cases}k=12,\\ m_1^2+n_1^2=41,\end{cases}$ $\begin{cases}k=16,\\ m_1^2+n_1^2=29,\end{cases}$ $\begin{cases}k=21,\\ m_1^2+n_1^2=9.\end{cases}$

由于55，51都是$4N+3$形状的数，不能表为两个平方的和，并且9也不能表成两个正整数的平方和，因此只有$k=12$与$k=16$时有正整数解m_1，n_1.

当$k=12$时，由$m_1^2+n_1^2=41$，得$(m_1,n_1)=(4,5)$，则$a=6m_1=24$，$b=6n_1=30$，$c=2k-1=23$，于是$(a,b,c)=(24,30,23)$.

当$k=16$时，由$m_1^2+n_1^2=29$，得$(m_1,n_1)=(2,5)$，这时$a=6m_1=12$，$b=6n_1=30$，$c=2k-1=31$，因此$(a,b,c)=(12,30,31)$.

(ii) 若 $3\nmid k(k+1)$时，由于任何三个连续数中必有一个是3的倍数，则 $k+1$ 是3的倍数，故 k 被3除余2，因此 k 只能取2，5，8，11，14，17，20诸值.

利用①式分别讨论如下：

若 $k=2$，则 $m_1^2+n_1^2=499$，而 $499\equiv3 \pmod 4$，此时无解.

若 $k=5$，则 $m_1^2+n_1^2=481$，利用关系式

$(\alpha^2+\beta^2)(x^2+y^2)=(\alpha x+\beta y)^2+(\alpha y-\beta x)^2=(\alpha x-\beta y)^2+(\alpha y+\beta x)^2$，

可知 $481=13\times37=(3^2+2^2)(6^2+1^2)=20^2+9^2=16^2+15^2$.

所以 $(m,n)=(9,20)$或$(15,16)$.

于是得两组解$(a,b,c)=(2m,2n,2k-1)=(18,40,9)$或$(30,32,9)$.

若 $k=8$，则 $m_1^2+n_1^2=445$，而 $445=5\times89=(2^2+1^2)(8^2+5^2)=21^2+2^2=18^2+11^2$，所以，$(m,n)=(2,21)$或$(11,18)$，得两组解$(a,b,c)=(2m,2n,2k-1)=(4,42,15)$或$(22,36,15)$.

若 $k=11$，有 $m_1^2+n_1^2=391$，而 $391\equiv3 \pmod 4$，此时无解.

若 $k=14$，有 $m_1^2+n_1^2=319$，而 $319\equiv3 \pmod 4$，此时无解.

若 $k=17$，有 $m_1^2+n_1^2=229$，而 $229=15^2+2^2$，得$(m,n)=(2,15)$，得一组解$(a,b,c)=(2m,2n,2k-1)=(4,30,33)$.

若 $k=20$，则 $m_1^2+n_1^2=121=11^2$，而 11^2 不能表示为两个正整数的平方和，因此本题共有7组解为：$(23,24,30)$，$(12,30,31)$，$(9,18,40)$，$(9,30,32)$，$(4,15,42)$，$(15,22,36)$，$(4,30,33)$.

经检验，它们都满足方程.

27. 本解答中的字母均表示整数.

令 $t=y^5$，由等式 $2x^2-1=y^{15}$ 推知

$t^3+1=(t+1)(t^2-t+1)=2x^2$.

由于 t^2-t+1 恒为奇数，所以或者 $t+1=2u^2$，$t^2-t+1=v^2$；或者 $t+1=6u^2$，$t^2-t+1=3v^2$. 这是因为，如果 $a=(t+1,\ t^2-t+1)$，那么 $a=1$ 或 $a=3$. 事实上，我们有 $t^2-t+1=(t-2)(t+1)+3$，由此可见，如果 d 是 t^2-t+1 和 $t+1$ 的公约数，那么 d 必是3的约数. 由于 $x>1$，所以 $t>1$，故有

$(t-1)^2<t^2-t+1<t^2$.

这表明等式 $t^2-t+1=v^2$ 不可能成立，所以只能有 $t+1=y^5+1=6u^2$.

另一方面，由于

$(y^5+1)-(y^3+1)=y^3(y-1)(y+1)$，

所以$(y^5+1)-(y^3+1)$可被3整除，因而 y^3+1 可被3整除，亦即 $y^3=3m-1$.

再记 $z=y^3=3m-1$. 又可由题中等式 $2x^2-1=y^{15}$，推知

$z^5+1=(z+1)(z^4-z^3+z^2-z+1)=2x^2$.

如果 $z^4-z^3+z^2-z+1$ 可被5整除，则立知题中结论成立. 否则，必有$(z+1,z^4-z^3+z^2-z+1)=1$，事实上，由 $z^4-z^3+z^2-z+1=(z^3-2z^2+3z-4)(z+1)+5$ 可知：如果 $b=(z+1,z^4-z^3+z^2-z+1)$，则 $b=1$ 或 $b=5$. 既然 $b\neq5$，所以 $b=1$. 于是再由 $z^4-z^3+z^2-z+1$ 为奇数，可知 $z+1=2u^2$，$z^4-z^3+z^2-z+1=v^2$. 但是由于 $z+1=3m$，所以等式 $z^4-z^3+z^2-z+1=v^2$ 的左端被3除余2，而其右端被3除的余数却是0或1，此为不可能.

28. 证法 1 将两式相加后等式两边都加上 1，得

$(x^3+y+1)^2+z^9=147^{157}+157^{147}+1.$ ①

对比 Fermat 小定理，我们对上式两边 mod 19，可知 $z^{18}\equiv0$ 或 1 (mod 19)，故 $z^9\equiv-1$，0 或 1 (mod 19).

而对任意 $a\in \mathbf{Z}$，有 $a\equiv0$，±1，±2，…，±9 (mod 19)，从而 $a^2\equiv0$，1，4，9，-3，6，-2，-8，7，5.

对比上述两个结论，可知①式左边满足：

$(x^3+y+1)^2+z^9\not\equiv-6,-5 \pmod{19}$.

而再由 Fermat 小定理，可知①式右边满足：

$$147^{157}+157^{147}+1\equiv14^{18\times8+13}+5^{18\times8+3}+1\equiv14^{13}+5^3+1\equiv-5^{13}+12$$
$$\equiv-5\times6^6+12\equiv-5\times(-2)^3+12\equiv52\equiv-5 \pmod{19}.$$

所以，①式左右两边不能相等.

从而，原方程没有整数解.

证法 2 获得证法一中的①式后也可选择两边模 13. 这时利用 Fermat 小定理，对任意 $a\in \mathbf{N}^*$，若 $13\nmid a$，则 $a^{12}\equiv1$ (mod 13)，知 $147^{157}\equiv4^1\equiv4$ (mod 13). 而 $157^{147}\equiv1^{147}\equiv1$ (mod 13)，故

$(x^3+y+1)^2+z^9\equiv6 \pmod{13}.$ ②

另一方面，由条件式中的第一个式子，知

$(x^3+1)(x^3+y)\equiv147^{157}\equiv4 \pmod{13}.$ ③

而立方数$\equiv0$，±1 或 ±5 (mod 13)，结合上式，可知 $x^3\not\equiv-1$ (mod 13)，所以，$x^3\equiv0$，1，5，或 -5，对比③可知对应地有 $x^3+y\equiv4$，2，5，-1 (mod 13)，从而

$(x^3+y+1)^2\equiv12,9,10$ 或 0 (mod 13). ④

再利用 z^9 是一个立方数，故 $z^9\equiv0$，1，5，8 或 12 (mod 13)，结合④就有

$(x^3+y+1)^2+z^9\not\equiv3$ 或 6 (mod 13).

这与②式矛盾.

注 这个解法表明将 z^9 改为 z^3 后，命题仍然成立.

29. 由题意知$(z-1)(z+1)=x^y$. 当 x 为奇数时，$(z-1,z+1)=1$；而当 x 为偶数时，$(z-1,z+1)=2$. 在前一种情况下，有 $z-1=u^y$，$z+1=v^y$，其中 u、v 为正整数，由此可得，$v^y-u^y=2$. 另一方面，由于 $v>u$，$y>1$，所以

$v^y-u^y=(v-u)(v^{y-1}+uv^{y-2}+\cdots+u^{y-1})\geqslant3$，

由此得出矛盾. 所以 x 为偶数. 此时 $z-1$ 与 $z+1$ 中有一者是 2 的倍数，但不是 4 的倍数；另一者则为 2^{y-1} 的倍数，却不是 2^y 的倍数. 这样一来，我们就有 $\{z-1, z+1\}=\{2u^y, 2^{y-1}v^y\}:=\{A, B\}$，其中 u 和 v 为奇数，“$:=$”表示“记为”. 显然 $AB=x^y$，$|A-B|=|2u^y-2^{y-1}v^y|=2\Rightarrow|u^y-2^{y-2}v^y|=1$. 这就是说，有 $2^{y-2}v^y=u^y+1$，或 $2^{y-2}v^y=u^y-1$.

我们指出 $u>1$. 事实上，如果 $u=1$，则 $A=2$，$A=z-1$，$z=3$，从而必有 $x=2$，与题意相矛盾. 此外，y 必为奇数. 因若不然，$y=2n$，那么就有 $z^2-x^{2n}=1$，此为不可能.

引理 1 如果 a 为不小于 2 的整数，p 为奇素数，那么 a^p-1 至少有一个素约数不能整

除$a-1$.

引理 1 的证明：我们有

$$a^p-1=(a-1)(a^{p-1}+a^{p-2}+\cdots+1):=(a-1)b.$$

我们首先来证明，$a-1$ 与 b 不可能有不同于 1 和 p 的公共素约数 q. 事实上，如果 $q\mid(a-1)$，那么对任何正整数 m，都有 $q\mid(a^m-1)$，因此

$$b=a^{p-1}+a^{p-2}+\cdots+1=\sum_{m=1}^{p-1}(a^m-1)+p=lq+p,$$

其中 l 是某个整数. 这就说明，只有在 q 等于 1 或 p 时，b 才能被 q 整除. 因此为完成引理的证明，只需再考查 $b=p^\alpha$，而且 $a-1$ 可被 p 整除的情形. 下证这是一种不可能出现的情形. 注意到 $b>p$，所以只要证明 b 不能被 p^2 整除. 下面我们加以证明.

如果 $a=p^\alpha k+1$，其中 k 不能被 p 整除，则有

$$a^p=(p^\alpha k+1)^p=1+p^{\alpha+1}k+p\cdot\frac{p-1}{2}\cdot p^{2\alpha}k^2+\cdots:=1+p^{\alpha+1}k+p^{2+\alpha}d,$$

其中 d 为整数，于是 $(a-1)b=a^p-1=p^{\alpha+1}(k+pd)$. 既然 k 不能被 p 整除，所以 b 只能被 p 整除，而不能被 p^2 整除.

引理 2　设 a 为不小于 2 的整数，p 为奇素数. 如果 $a\neq2$ 或 $p\neq3$，那么 a^p+1 至少有一个素约数不能整除 $a+1$.

引理 2 的证明：我们有

$$a^p+1=(a+1)(a^{p-1}-a^{p-2}+\cdots+a^2-a+1):=(a-1)b.$$

首先证明，$a+1$ 与 b 不可能有不同于 1 和 p 的公共素约数 r. 事实上，如果 $r\mid(a+1)$，那么对任何奇数 k，都有 $r\mid(a^k+1)$；而当 $k=2m$ 时，则因有 $(a^2-1)\mid(a^{2m}-1)$，$r\mid(a^2-1)$，所以 $r\mid(a^{2m}-1)$. 这样一来，就有 $b=lr+p$，其中 l 为某个整数. 所以只有在 r 等于 1 或 p 时，b 才能被 r 整除.

这样一来，为完成引理的证明，只需再考察 $b=p^\alpha$，而且 $a+1$ 可被 p 整除的情形. 下证这是一种不可能出现的情形. 证法与引理 1 类似，先证 $b>p$. 事实上，我们有 $b\geqslant a^2-a+1\geqslant a+1\geqslant p$. 而由题中条件可知，在这一连串不等号中至少有一个为严格大于号. 另一方面，如同引理 1 那样，可以证得：b 不能被 p^2 整除，从而得出矛盾. 引理 2 证毕.

现在证明题目本身. 考察已得的等式 $u^y\pm1=2^{y-2}v^y$. 由所证的引理可知，该式右端有不少于 $q+1$ 个不同的素约数. 既然 $(u, 2v)=1$，$u>1$，所以题中断言成立.

注　事实上，这里证明了一个比题中断言更强的结论：如果 y 可以表示为 n 个大于 1 的整数的乘积，那么 x 至少有 $n+2$ 个不同的素约数.

30. 显然 $n\neq1$.

当 $n=2k$ 为偶数时，令 $x_{2i-1}=1$，$x_{2i}=-1$ $(i-1, 2, \cdots, k)$，$y=1$，则满足条件.

当 $n=3+2k$ $(k\in\mathbf{N}_+)$ 时，令

$$y=2,\ x_1=4,\ x_2=x_3=x_4=x_5=-1,\ x_{2i}=2,\ x_{2i+1}=-2,\ i=3, 4, \cdots, k+1,$$

则满足条件.

当 $n=3$ 时，若存在非零整数 x_1，x_2，x_3，使得

$$\begin{cases}x_1+x_2+x_3=0,\\ x_1^2+x_2^2+x_3^2=3y^2,\end{cases}$$

则 $2(x_1^2+x_2^2+x_1x_2)=3y^2$.

不妨设 $(x_1, x_2)=1$，则 x_1，x_2 都是奇数或者一奇一偶，从而 $x_1^2+x_2^2+x_1x_2$ 是奇数. 另一方面 $2\mid y$，故 $3y^2\equiv 0 \pmod 4$，而 $2(x_1^2+x_2^2+x_1x_2)\equiv 2 \pmod 4$，矛盾!

综上所述，满足条件的正整数 n 为除了 1 和 3 外的一切正整数.

31. 我们的证明需要下面的引理.

引理 设 p 是一个给定的奇素数，整数 $u>1$ 且 $p\nmid u$. 设 d 是 u 模 p 的阶，并设 $p^v \| (u^d-1)$，则对任意与 p 互素的正整数 m 及任意整数 $t\geqslant 0$，有 $p^{t+v} \| (u^{dmp^t}-1)$.

引理的证明：对 t 归纳，当 $t=0$ 时，由 v 的定义知 $u^d=1+p^vk$（其中 $p\nmid k$），故由二项式定理得

$$u^{md}=(1+p^vk)^m=1+p^vkm+p^{2v}k^2C_m^2+\cdots=1+p^v(km+p^vk^2C_m^2+\cdots).$$

由于 $p\nmid km$ 及 $v\geqslant 1$，故上式右端可表示为 $1+p^vk_1$ 的形式，其中 k_1 是一个与 p 互素的整数，从而引理在 $t=0$ 时成立.

假设引理对 t 已成立，即设 $u^{dmp^t}=1+p^{t+v}k_t$，其中 $p\nmid k_t$，则由二项式定理知

$$u^{dmp^{t+1}}=(1+p^{t+v}k_t)^p=1+p^{t+1+v}(k_t+C_p^2p^{v+t-1}k_t^2+\cdots)=1+p^{t+1+v}k_{t+1},$$

其中 $p\nmid k_{t+1}$（注意 p 是奇素数，故 $p\mid C_p^2$）.

这就完成了引理的归纳证明.

现在证明本题的结论.

当 $u=1$ 时结论显然成立.

对 $u>1$，将方程化为

$$n!=u^r(u^s-1), \tag{①}$$

其中 r、s 为正整数.

取定一个奇素数 $p\nmid u$，可设 $n>p$（否则结论已成立.）并设 $p^\alpha \| n!$，则 $\alpha\geqslant 1$. 由①及 $p\nmid u$ 知 $p^\alpha \| (u^s-1)$，特别地有 $p\mid (u^s-1)$. 设 d 是 u 模 p 的阶，则有 $d\mid s$. 设 $s=dmp^t$，其中 $t\geqslant 0$，$p\nmid m$，则由 $p^\alpha \| (u^s-1)$ 及引理可知 $\alpha=t+v$，即 $t=\alpha-v$. 故

$$u^s-1=u^{dmp^{\alpha-v}}-1. \tag{②}$$

熟知

$$\alpha=\sum_{l=1}^{\infty}\left[\frac{n}{p^l}\right]\geqslant\left[\frac{n}{p}\right]>an, \tag{③}$$

其中 a 是一个仅与 p 有关的正常数，记 $b=u^{dp^{-v}}$.

由于 d，p，u，v 均是固定的正整数，故 b 是大于 1 的常数，因此由②，③得

$$u^s-1\geqslant u^{dp^{\alpha-v}}-1>b^{p^{an}}-1. \tag{④}$$

但当 n 充分大时，易知

$$b^{p^{an}}-1>n^n-1 \tag{⑤}$$

（此即 $b^{p^{an}}\geqslant n^n$，即 $p^{an}>n\log_b n$）. 故由②，④，⑤知，当 n 充分大时，有 $u^s-1>n!$，更有 $u^r(u^s-1)>n!$. 故 n 充分大后方程①无解. 另一方面，对任一个固定的 n，方程①显然至多有有限组解 (r, s)，从而问题中的方程至多有有限组正整数解 (n, a, b).

32. 对正整数 x，y，有

$x \mid y^2+210$，$y \mid x^2+210$，$(x,y)=1$

$\Leftrightarrow xy \mid x^2+y^2+210$，$(x,y)=1$

$\Leftrightarrow x^2+y^2+210=kxy$，$(x,y)=1$，$k$ 为某个正整数.

易知，$(x,y)=1$，$(x,210)=1$，$(y,210)=1$ 中由任一个出发可导出另两个，且 $k\geqslant 3$.

若 $x=y$，易知 $x=y=1$，$k=212$.

若 $x=1$，则 $k=y+\frac{211}{y}$，注意到 211 是素数，故 $y=1$ 或 211，$k=212$.

若 $1<x<y$，先证：$x\geqslant 15$.

假设 $x\leqslant 14$，由于 $(x,210)=1$，故 $x=11$ 或 13.

如果 $x=11$，则 $y^2+331=k\cdot y\cdot 11$，注意到 331 是素数，故 $y=331$，从而 $11 \mid 332$，矛盾.

如果 $x=13$，则 $y^2+379=k\cdot y\cdot 13$，注意到 379 是素数，故 $y=379$，从而 $13 \mid 380$，矛盾.

当 $x\geqslant 15$ 时，将方程变形为：

$y^2-kxy+(x^2+210)=0$.

设方程的另一根为 y'，则有

$y+y'=kx$，

$y\cdot y'=x^2+210$.

易知 $y'\in \mathbf{Z}^+$.

由于 $x^2>210$，故

$(y-x)^2+x^2>(y-x)^2+210=(k-2)xy\geqslant xy$，

$(y-x)^2>x(y-x)$.

由于 $y-x>0$，故 $y-x>x$，即 $y>2x$. 从而

$$y'=\frac{x^2+210}{y}<\frac{x^2+210}{2x}<\frac{x^2+x^2}{2x}=x.$$

所以 (y',x) 是一组"更小"的解，且 k 值不变.

这就是说，每一组 $(x,y)(1<x<y)$ 都可以由 $(1,1)$ 或 $(1,211)$ 导出，且 $k=212$. 由于 $(1,211)$ 也可由 $(1,1)$ 导出，所以可构造数列 $\{a_n\}$ 如下：$a_1=a_2=1$，$a_{n+2}=212a_{n+1}-a_n$，则原方程的所有正整数解为 (a_n,a_{n+1}) 和 (a_{n+1},a_n)，$n\in \mathbf{Z}^+$.

33. (1) 先证一个引理：

引理 1　不存在不全为零的整数 a，b，c，使得

$$a^2+b^2+c^2=kabc, \qquad ①$$

其中 k 是某个偶整数.

引理 1 的证明：假设不然，设 (a,b,c) 是使 $|a|+|b|+|c|$ 达最小的不全为零的整数组，注意到 k 为偶数，故 a，b，c 中必有偶数，从而 $a^2+b^2+c^2\equiv 0 \pmod 4$.

由于整数的平方模 4 的余数为 0 或 1，故 a，b，c 只能都为偶数. 设 $a=2a_1$，$b=2b_1$，$c=2c_1$，其中 a_1，b_1，c_1 是整数，代入①式得：

$a_1^2+b_1^2+c_1^2=2ka_1b_1c_1$，

但 $0<|a_1|+|b_1|+|c_1|=\frac{1}{2}(|a|+|b|+|c|)<|a|+|b|+|c|$，矛盾！

回到原题. 固定 k，设 (a, b, c) 是使得 $a+b+c$ 达最小的正整数解，不妨设 $a\leqslant b\leqslant c$.

将①式改写为：$c^2-kabc+(a^2+b^2)=0$.

设另一根为 c'，则

$c+c'=kab, c\cdot c'=a^2+b^2$.

易知 $c'\in \mathbf{Z}^+$. 由 $a+b+c'\geqslant a+b+c$ 得，$c'\geqslant c$，则

$c^2\leqslant cc'=a^2+b^2<(a+b)^2$，即 $c<a+b$.

从而 $k=\frac{a^2+b^2+c^2}{abc}=\frac{a}{bc}+\frac{b}{ca}+\frac{c}{ab}\leqslant\frac{1}{c}+\frac{1}{a}+\frac{c}{ab}<\frac{1}{c}+\frac{1}{a}+\frac{a+b}{ab}=\frac{2}{a}+\frac{1}{b}+\frac{1}{c}\leqslant 4$.

由于 $(a,b,c)=(1,1,1)$ 时，$k=3$；$(a,b,c)=(3,3,3)$ 时，$k=1$. 又结合引理知，$k=1$ 或 3.

(2) 先考虑 $k=3$.

定义数列 $\{F_n\}$ 如下：

$F_0=0, F_1=1, F_{n+2}=F_{n+1}+F_n$.

引理 2 (i) $F_{n+1}F_{n-1}-F_n^2=(-1)^n$ $(n\geqslant 1)$，特别地 $F_{2n+1}\cdot F_{2n-1}=F_{2n}^2+1$.

(ii) $F_{n+m}=F_nF_{m-1}+F_mF_{n+1}$ $(n\geqslant 0, m\geqslant 1)$，特别地，$F_{2n+1}=F_n^2+F_{n+1}^2$.

(iii) $1+F_{2n-1}^2+F_{2n+1}^2=3F_{2n-1}F_{2n+1}$ $(n\geqslant 1)$.

引理 2 的证明：(i) 定义 $x_n=F_{n+1}F_{n-1}-F_n^2$，则 $x_1=-1$.

$x_{n+1}=F_{n+2}F_n-F_{n+1}^2=(F_{n+1}+F_n)F_n-F_{n+1}^2=F_n^2-F_{n+1}(F_{n+1}-F_n)$

$=F_n^2-F_{n+1}F_{n-1}=-x_n$，

由此易得 $x_n=(-1)^n$.

(ii) 对 n 归纳，其中 m 是任意正整数.

当 $n=0$ 时，$F_0F_{m-1}+F_mF_{0+1}=F_m=F_{0+m}$.

假设命题对 n 成立，考察 $n+1$.

由归纳假设和 F_n 的递推关系，

$F_{(n+1)+m}=F_{n+(m+1)}=F_nF_m+F_{m+1}F_{n+1}=F_m(F_{n+2}-F_{n+1})+F_{n+1}(F_m+F_{m-1})$

$=F_{n+1}F_{m-1}+F_mF_{(n+1)+1}$.

(iii) 当 $n=1$ 时，$1+F_1^2+F_3^2=6=3F_1F_3$.

假设 $1+F_{2n-1}^2+F_{2n+1}^2=3F_{2n-1}\cdot F_{2n+1}$，即 F_{2n-1} 是方程 $x^2-3F_{2n+1}x+(F_{2n+1}^2+1)=0$ 的一根，另一根为 $3F_{2n+1}-F_{2n-1}=2F_{2n+1}+F_{2n}=F_{2n+1}+F_{2n+2}=F_{2n+3}$. 从而

$1+F_{2n+1}^2+F_{2n+3}^2=3\cdot F_{2n+1}\cdot F_{2n+3}$.

由引理 2 知，$(a,b,c)=(1,F_{2n-1},F_{2n+1})$ $(n\geqslant 2)$ 是方程①的正整数解，且有：

$1\cdot F_{2n-1}=F_{n-1}^2+F_n^2$，$1\cdot F_{2n+1}=F_n^2+F_{n+1}^2$，$F_{2n-1}\cdot F_{2n+1}=F_{2n}^2+1^2$.

对 $k=1$，由前面讨论已知，存在无穷多个正整数组 (a_n, b_n, c_n) 满足 $a_n^2+b_n^2+c_n^2=3a_nb_nc_n$，且 a_n，b_n，c_n 中任两数之积都可表为两个正整数的平方和，则易知 $3a_n$，$3b_n$，$3c_n$ 中任两数之和也都可表为两个正整数的平方和，且

$(3a_n)^2+(3b_n)^2+(3c_n)^2=(3a_n)(3b_n)(3c_n)$.

34. 证法 1 首先我们证明如下一个引理.

引理 不定方程

$$x^2+11y^2=4m \quad ①$$

或有奇数解 (x_0, y_0)，或有满足

$$x_0\equiv(2k+1)y_0 \pmod m \quad ②$$

的偶数解 (x_0, y_0).

引理的证明：考虑如下表示：$x+(2k+1)y$，x，y 为整数，且 $0\leqslant x\leqslant 2\sqrt{m}$，$0\leqslant y\leqslant\frac{\sqrt{m}}{2}$，则共有 $([2\sqrt{m}]+1)\left(\left[\frac{\sqrt{m}}{2}\right]+1\right)>m$ 个表示，因此存在整数 x_1，$x_2\in[0, 2\sqrt{m}]$，y_1，$y_2\in\left[0, \frac{\sqrt{m}}{2}\right]$，满足 $(x_1, y_1)\neq(x_2, y_2)$，且

$$x_1+(2k+1)y_1\equiv x_2+(2k+1)y_2 \pmod m,$$

这表明

$$x\equiv(2k+1)y \pmod m, \quad ③$$

这里 $x=x_1-x_2$，$y=y_2-y_1$. 由此可得

$$x^2\equiv(2k+1)^2y^2\equiv-11y^2 \pmod m,$$

故 $x^2+11y^2=km$. 因为 $|x|\leqslant2\sqrt{m}$，$|y|\leqslant\frac{\sqrt{m}}{2}$，所以

$$x^2+11y^2<4m+\frac{11}{4}m<7m,$$

于是 $1\leqslant k\leqslant6$. 因为 m 为奇数，$x^2+11y^2=2m$，$x^2+11y^2=6m$ 显然没有整数解.

(1) 若 $x^2+11y^2=m$，则 $x_0=2x$，$y_0=2y$ 是方程①满足②的解.

(2) 若 $x^2+11y^2=4m$，则 $x_0=x$，$y_0=y$ 是方程①满足②的解.

(3) 若 $x^2+11y^2=3m$，则 $(x\pm11y)^2+11(x\mp y)^2=3^2\cdot4m$.

首先假设 $3\nmid m$，若 $x\not\equiv0 \pmod 3$，$y\not\equiv0 \pmod 3$，且 $x\not\equiv y \pmod 3$，则

$$x_0=\frac{x-11y}{3},\ y_0=\frac{x+y}{3} \quad ④$$

是方程①满足②的解. 若 $x\equiv y\not\equiv0 \pmod 3$，则

$$x_0=\frac{x+11y}{3},\ y_0=\frac{y-x}{3} \quad ⑤$$

是方程①满足②的解.

现在假设 $3\mid m$，则公式④和⑤仍然给出方程①的整数解. 若方程①有偶数解 $x_0=2x_1$，$y_0=2y_1$，则

$$x_1^2+11y_1^2=m\Leftrightarrow36m=(5x_1\pm11y_1)^2+11(5y_1\mp x_1)^2.$$

因为 x_1、y_1 的奇偶性不同，所以 $5x_1\pm11y_1$，$5y_1\mp x_1$ 都为奇数.

若 $x\equiv y \pmod 3$，则 $x_0=\frac{5x_1-11y_1}{3}$，$y_0=\frac{5y_1+x_1}{3}$ 是方程①的一奇数解.

若 $x_1\not\equiv y_1 \pmod 3$，则 $x_0=\frac{5x_1+11y_1}{3}$，$y_0=\frac{5y_1-x_1}{3}$ 是方程①的一奇数解.

(4) $x^2+11y^2=5m$，则

$5^2 \cdot 4m=(3x\mp 11y)^2+11(3y\pm x)^2$.

当 $5\nmid m$ 时，若 $x\equiv\pm 1 \pmod 5$，$y\equiv\mp 2 \pmod 5$，或 $x\equiv\pm 2 \pmod 5$，$y\equiv\pm 1 \pmod 5$，则

$$x_0=\frac{3x-11y}{5},\quad y_0=\frac{3y+x}{5} \qquad ⑥$$

是方程①满足②的解.

若 $x\equiv\pm 1 \pmod 5$，$y\equiv\pm 2 \pmod 5$，或 $x\equiv\pm 2 \pmod 5$，$y\equiv\mp 1 \pmod 5$，则

$$x_0=\frac{3x+11y}{5},\quad y_0=\frac{3y-x}{5} \qquad ⑦$$

是方程①满足②的解.

当 $5\mid m$，则公式⑥和⑦仍然给出方程①的整数解. 若方程①有偶数解 $x_0=2x_1$，$y_0=2y_1$，则

$$x_1^2+11y_1^2=m,\ x_1\not\equiv y_1 \pmod 2),$$

可得 $100m=(x_1\mp 33y_1)^2+11(y_1\pm 3x_1)^2$.

若 $x_1\equiv y_1\equiv 0 \pmod 5$，或者 $x_1\equiv\pm 1 \pmod 5$，$y_1\equiv\pm 2 \pmod 5$，或者 $x_1\equiv\pm 2 \pmod 5$，$y_1\equiv\mp 1 \pmod 5$，则 $x_0=\frac{x_1-33y_1}{5}$，$y_0=\frac{y_1+3x_1}{5}$ 是方程①的一奇数解.

若 $x_1\equiv\pm 1 \pmod 5$，$y_1\equiv\mp 2 \pmod 5$，或 $x_1\equiv\pm 2 \pmod 5$，$y_1\equiv\pm 1 \pmod 5$，则

$$x_0=\frac{x_1+33y_1}{5},\quad y_0=\frac{y_1-33x_1}{5}$$

是方程①的一奇数解.

引理证毕.

由引理，若方程①没有奇数解，则它有一个满足②的偶数解 (x_0,y_0). 令 $l=2k+1$，考虑二次方程

$$mx^2+ly_0x+ny_0^2-1=0, \qquad ⑧$$

则 $x=\frac{-ly_0\pm\sqrt{l^2y_0^2-4mny_0^2+4m}}{2m}=-\frac{ly_0\pm x_0}{2m}$,

这表明方程⑧至少有一个整数根 x_1，即

$$mx_1^2+ly_0x_1+ny_0^2-1=0, \qquad ⑨$$

上式表明 x_1 必为奇数. 将⑨乘以 $4n$ 后配方得

$$(2ny_0+lx_1)^2+11x_1^2=4n,$$

这表明方程 $x^2+11y^2=4n$ 有奇数解 $x=2ny_0+lx_1$，$y=x_1$.

证法 2　首先证明如下引理.

引理　令 m、n、t 是三个正整数，满足 $t^2+11=4mn$，则存在整数 u，v，x，y，使得下面三式之一成立：

（Ⅰ）当 u、v 为奇数时，有 $\begin{cases}4m=u^2+11v^2,\\ n=x^2+11y^2,\\ t=ux+11vy,\\ |uy-vx|=1;\end{cases}$

(Ⅱ)当 x、y 为奇数时，有 $\begin{cases} m=u^2+11v^2, \\ 4n=x^2+11y^2, \\ t=ux+11vy, \\ |uy-vx|=1; \end{cases}$

(Ⅲ)当 u、v 为奇数，且 x、y 为奇数时，有 $\begin{cases} 4m=u^2+11v^2, \\ 4n=x^2+11y^2, \\ t=\dfrac{ux+11vy}{2}, \\ |uy-vx|=2. \end{cases}$

引理的证明，我们对 t 用归纳法.

当 $t=1$ 时，$(m, n)=(1, 3)$，$(3, 1)$. 前者可取 $u=1$，$v=0$，$x=y=1$，属于(Ⅱ). 后者可取 $u=v=1$，$x=1$，$y=0$，属于(Ⅰ). 现在假设结论对小于 t 的自然数成立. 不防设 $m\leqslant n$. 若 $m=n$，$4m^2-t^2=11\Rightarrow m=n=3$，$t=5$. 此时可取 $u=v=1$，$x=-1$，$y=1$，(Ⅲ)成立. 若 $m=1$，则可取 $u=1$，$v=0$，$x=t$，$y=1$，(Ⅱ)成立. 下设 $1<m<n$，$n\geqslant m+2\Rightarrow t^2+11\geqslant 4m(m+2)>(2m)^2+11\Rightarrow t>2m$.

$4mn=t^2+11\Rightarrow 4m(m+n-t)=(t-2m)^2+11$,

$m+n\geqslant\sqrt{4mn}>t$，$0<t-2m<t$.

由归纳法假设，(Ⅰ)，(Ⅱ)，(Ⅲ)之一对 $(m, m+n-t, t-2m)$ 成立.

如果对 $(m, m+n-t, t-2m)$，(Ⅰ)成立，则存在整数 u，v，x，y，使得

$$\begin{cases} 4m=u^2+11v^2, \\ m+n-t=x^2+11y^2, \\ t-2m=ux+11vy, \\ |uy-vx|=1, \end{cases} \quad (u, v\text{为奇数}).$$

从上式中解出 m，n，t 得

$$\begin{cases} 4m=u^2+11v^2, \\ 4n=(2x+u)^2+11(2y+v)^2, \\ t=\dfrac{u(2x+u)+11v(2y+v)}{2}, \\ |u(2y+v)-v(2x+u)|=2|uy-vx|=2, \end{cases} \quad (u, v\text{为奇数}).$$

即对 (m, n, t)，(Ⅲ)成立.

如果对 $(m, m+n-t, t-2m)$，(Ⅱ)成立，则存在整数 u，v，x，y，使得

$$\begin{cases} m=u^2+11v^2, \\ 4(m+n-t)=x^2+11y^2, \\ t-2m=ux+11vy, \\ |uy-vx|=1, \end{cases} \quad (x, y\text{为奇数}).$$

从上式中解出 m，n，t 得

$$\begin{cases} m=u^2+11v^2, \\ 4n=(x+2u)^2+11(y+2v)^2, \\ t=u(x+2u)+11v(y+2v), \\ |u(y+2v)-v(x+2u)|=|uy-vx|=1, \end{cases} \quad (u,\ v\text{为奇数}).$$

即对 $(m,\ n,\ t)$，(Ⅱ) 成立.

如果对 $(m,\ m+n-t,\ t-2m)$，(Ⅲ) 成立，则存在整数 u，v，x，y，使得

$$\begin{cases} 4m=u^2+11v^2, \\ 4(m+n-t)=x^2+11y^2, \\ t-2m=\dfrac{ux+11vy}{2}, \\ |uy-vx|=2, \end{cases} \quad (u,\ v\text{为奇数；}x,\ y\text{为奇数}).$$

从上式中解出 m，n，t 得

$$\begin{cases} 4m=u^2+11v^2, \\ n=\left(\dfrac{x+u}{2}\right)^2+11\left(\dfrac{y+v}{2}\right)^2, \\ t=u\left(\dfrac{x+u}{2}\right)+11v\left(\dfrac{y+v}{2}\right), \\ \left|u\left(\dfrac{y+v}{2}\right)-v\left(\dfrac{x+u}{2}\right)\right|=\dfrac{|uy-vx|}{2}=1, \end{cases} \quad (u,\ v\text{为奇数}).$$

即对 $(m,\ n,\ t)$，(Ⅰ) 成立. 引理证毕.

对 $t=2k+1$ 应用上述引理立得本题结论.

第十八章　整点

1. 设 $x=5n+r$，其中 n 是整数，$r\in\{0,1,2,3,4\}$则

$y=\frac{1}{5}[(5n+r)^2-(5n+r)+1]=5n^2+(2r-1)n+\frac{1}{5}(r^2-r+1)$.

当 $r=0$，1，2，3，4 时，

$r^2-r+1=1$，1，3，7，13，均不是 5 的倍数. 因而$\frac{1}{5}(r^2-r+1)$不是整数，

而 $5n^2+(2r-1)n$ 是整数，

于是，对任意的整数 x，y 都不可能取整数，因此，曲线 $y=\frac{1}{5}(x^2-x+1)$不可能经过整点.

2. (1) 设 l 是一条具有有理斜率的直线，则其方程可以写为

$ax+by+c=0$，

其中 a 和 b 都是整数，且 $b\neq 0$.

设(x_1,y_1)是直线 l 上的一个整点，则

$ax_1+by_1+c=0$.

且又有

$a(x_1+kb)+b(y_1-ka)+c=ax_1+by_1+c=0$，

因此，形为(x_1+kb, y_1-ka)，$k\in\mathbf{Z}$的整点全在直线l上.

所以，如果在具有有理斜率的一条直线上有一个整点，则在它上面就有无穷多个整点；

(2) 设(p,q)为一整点，则(p,q)到直线$l: ax+by+c=0$的距离为

$$d_0=\frac{|ap+bq+c|}{\sqrt{a^2+b^2}}.$$

因为a，b，p，q均为整数，则$ap+bq$为整数.

若c为整数，则

$$d_0=0 \text{ 或 } d_0\geqslant\frac{1}{\sqrt{a^2+b^2}}. \quad ①$$

若c不是整数，设e是与c最接近的整数，则

$$d_0\geqslant\frac{|e-c|}{\sqrt{a^2+b^2}}. \quad ②$$

由于(p, q)是任意的，则存在d使之不满足①，②$(d\neq0)$，即存在正数d，使得没有直线l之外的整点与该直线的距离小于d.

3. 分别以A和B表示红点和蓝点的集合.

假设结论不成立，即A中仅有有限个点其坐标为a的倍数，且B中仅有有限个点其坐标是b的倍数，这样在整个自然数集合中，就仅有有限个数是ab的倍数，这是不可能的.

4. 以圆心为坐标原点，并使坐标轴平行于方格线，在方格纸上建立坐标系，则所有结点均为整点.

如果点(x, y)落在圆周上，由对称性，一切形如$(\pm x, \pm y)$和$(\pm y, \pm x)$的点也落在圆周上，若$x\neq y$且$xy\neq0$，则这样的点共有8个，若$x=y$或$xy=0$，则这样的点共有4个.

由于 $1988\equiv4 \pmod 8$，

所以给定的1988个点中必有满足$x=y$的点或满足$xy=0$的点.

若存在满足$x=y$的点，则由$x^2+y^2=2x^2=R^2$可知，$\frac{R}{\sqrt2}$是整数，从而$\sqrt2R$是整数.

若存在满足$xy=0$的点，则由$R=|x|$或$R=|y|$可知，R是整数.

5. 记$1970=p$.

设(x_1, y_1)与$(x_i, y_i)(i=2,3)$三个整点所共线的既约方程为$ax+by=c$，其中a,b,c为整数.

若$p|a$，$p|b$，则必有$p|c$，由此可设$p\nmid b$.

因为$ax_1+by_1=c$，$ax_i+by_i=c(i=2,3)$，所以

$$a(x_1-x_i)=b(y_i-y_1), \quad ①$$

$$a(x_3-x_2)=b(y_2-y_3). \quad ②$$

根据题设 $x_1y_1=1+k_1p$，

$$x_iy_i=1+k_ip, (i=2,3), \quad ③$$

所以 $x_iy_i=x_1y_1+(k_i-k_1)p$.

于是有 $(x_1-x_i)by_i=bx_1y_i-bx_iy_i=bx_1y_i-bx_1y_1-b(k_i-k_1)p$

$$=bx_1(y_i-y_1)-b(k_i-k_1)p=ax_1(x_1-x_i)-b(k_i-k_1)p,$$

即 $(x_1-x_i)(ax_1-by_i)=b(k_i-k_1)p$.

由此可见，若 $p\nmid(x_1-x_2)$，则 $p|(ax_1-by_2)$，

若 $p\nmid(x_1-x_3)$，则 $p|(ax_1-by_3)$，

因此，若 $p\nmid(x_1-x_2)(x_1-x_3)$，则

$p|b(y_2-y_3)$.

因为 $p\nmid b$，则 $p|(y_2-y_3)$.

所以 $p|x_2(y_2-y_3)$.

又由③，$p|(1-x_2y_2)$，$p|(x_3y_3-1)$.

将以上三式相加得

$p|(x_3-x_2)y_3$.

由③，显然，$p\nmid y_3$，于是

$p|(x_3-x_2)$.

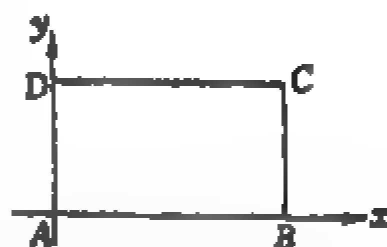
同理，若 $p\nmid(x_3-x_2)$，则 $p|(x_1-x_2)$或 $p|(x_1-x_3)$.

因此，x_1-x_2，x_1-x_3，x_3-x_2 三者至少有一个能被 p 整除.

由①，②，若 $p|(x_j-x_i)$，则 $p|(y_j-y_i)$.

于是本题得证.

6. 设 R 为矩形 $ABCD$.



以 A 为原点，AB 所在直线为 x 轴，AD 所在直线为 y 轴建立直角坐标系.

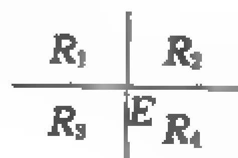
为证明 R 至少有一条边长为整数，只要证明 B，C，D 中至少有一个是整点即可.

因为每一个小矩形 R_i 至少有一条边长为整数，且它的边与坐标轴平行，所以 R_i 的顶点中整点的个数为 0，2 或 4.

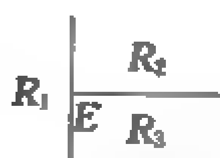
所以所有 R_i 的顶点中，整点的个数为偶数．这里一个顶点如果同时是 k 个，R_i 的顶点，则被计算 k 次.

A 是整点，并且只被计算 1 次.

如图，矩形 $ABCD$ 内部的整点 E 可能被计算 4 次，也可能被计算 2 次，于是内部顶点中整点的个数是偶数.



(E 被计算 4 次)





(E 被计算 2 次)

又由于整点的总个数是偶数，R 内部的整点个数为偶数，R 的顶点 A 被计算 1 次，所以 B，C，D 中至少有一个是整点.

因此，R 至少有一条边长为整数.

7. $n=3k$，$n=5k$，$k\in \mathbf{N}_+$.

显然，当 $n=3k(5k)$时，$n\times n$ 的方格表能分成k^2 个 $3\times3(5\times5)$的单元．因为任一单元中所有

整数之和为偶数，所以，$n\times n$ 的方格表中所有整数之和也是偶数.

下面举例证明：若 n 既不是 3 的倍数，也不是 5 的倍数，那么，方格表中所有整数之和可能为奇数.

考虑数列：

1011011011… ①

和 100011000110001100011000 1…. ②

以上两数列分别以三位和五位为周期. 设 A_k、B_k 分别是数列①、②的前 k 项的和. 显见，对任意的 k、$m\in\mathbf{N}_+$，有

$A_{k+15m}\equiv A_k \pmod 2$，$B_{k+15m}\equiv B_k \pmod 2$.

将 0 和 1 按以下规则填入 $n\times n$ 的方格表中：

若①的第 k 项是 1，就在方格表的第 k 列填入②的前 n 项；

若①的第 k 项是 0，就在方格表的第 k 列全填 0，易证方格表中数的总和等于 A_nB_n. 记

$A_1=1$，$A_2=1$，$A_4=3$，$A_7=5$，$A_8=5$，$A_{11}=7$，$A_{13}=9$，$A_{14}=9$，

$B_1=1$，$B_2=1$，$B_4=1$，$B_7=3$，$B_8=3$，$B_{11}=5$，$B_{13}=5$，$B_{14}=5$.

因此，若 $n\neq 3k$ 且 $n\neq 5k$ $(k\in\mathbf{N}_+)$，则 $n\times n$ 的方格表中数之和为奇数.

1	0	1	1	0	1	1
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
1	0	1	1	0	1	1
1	0	1	1	0	1	1
0	0	0	0	0	0	0

检验知，任一 3×3 和 5×5 的方格表中数字之和为偶数. 右表所示为 7×7 的方格表所举例子.

8. 首先，我们取坐标为 $(i,j,k)(i,j,k\in\{0,1\})$ 的八个格点，以这 8 个整点为顶点可以得到一个单位立方体，而这个单位立方体显然满足题设要求，故所求的最小值不小于 8. 另一方面，每个整点的三个坐标按奇偶性可以分为如下八类：

(奇，奇，奇)、(奇，奇，偶)、(奇，偶，奇)、(奇，偶，偶)，

(偶，奇，奇)、(偶，奇，偶)、(偶，偶，奇)(偶，偶，偶).

如果这个多面体有 9 个顶点，由抽屉原则，必有两个顶点属于同一类整点，则这两个顶点连线的中点也是整点，由多面体的凸性知，该整点属于这个多面体，与已知矛盾. 故所求的顶点个数不大于 8.

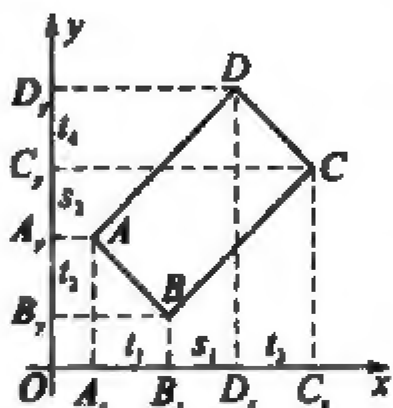
综上，该凸多面体最多有 8 个顶点.

9. 不可能.

解法 1 如右图，假设存在矩形 $ABCD$，它的各条边都刚好穿过奇数条方格线. 不妨设 AB 是它的较短边. 选择一个直角坐标系，它的原点位于某个结点上，它的坐标轴位于方格线上，使得在矩形的各个顶点中，顶点 A 的横坐标最小，顶点 B 的纵坐标最小. 分别以 A_x，B_x，C_x，D_x 和 A_y，B_y，C_y，D_y 表示各个顶点在 x 轴与 y 轴上的投影.

由于顶点 A，B，C，D 均不在方格线上，所以，点 A_x，B_x，C_x，D_x 的横坐标和点 A_y，B_y，C_y，D_y 的纵坐标都不是整数. 注意到 $A_xB_x=D_xC_x$ 和 $A_xD_x=AD\cdot\cos 45°\geqslant AB\cos 45°=A_xB_x$，

所以，四个顶点在 x 轴上的投影按 A_x，B_x，D_x，C_x 的顺序排列（点 B_x 与 D_x 可能重合）．同理，四个顶点在 y 轴上的投影按 B_y，A_y，C_y，D_y 的顺序排列．同时，有



$A_xB_x=D_xC_x=B_yA_y=C_yD_y=AB\cos 45°$，

$B_xD_x=A_yC_y=(AD-AB)\cos 45°$．

分别用 t_1，t_2，t_3，t_4，s_1，s_2 表示线段 A_xB_x，B_yA_y，D_xC_x，C_yD_y，B_xD_x，A_yC_y 上的坐标为整数的点的个数．由于在线段 A_xB_x 上恰好有 t_1 个坐标为整数的点，所以，边 AB 恰与 t_1 条纵向的方格线相交．同理，由于在线段 A_yD_y 上有 t_4+s_2 个坐标为整数的点，所以，边 AD 恰与 t_4+s_2 条横向的方格线相交．其他线段类似．

综上可知，矩形的每条边与奇数条方格线相交等价于以下各数都是奇数：

t_1+t_2，t_3+t_4，$t_1+t_4+s_1+s_2$，$t_2+t_3+s_1+s_2$．

引理　如果数轴上的两条线段的长度都是 d，并且它们的端点的坐标都不是整数，那么，它们上面的整点的数目至多相差 1．

事实上，若线段的左端点位于非整数 a 处，右端点位于非整数 b 处，且它上面有 k 个整点 n，$n+1$，…，$n+k-1$，则

$n-1<a<n$，$n+k-1<b<n+k$．

因此，$k-1<d=b-a<k+1$．

于是，$d-1<k<d+1$．

从而，$k=[d]$ 或 $k=[d]+1$．

引理得证．

由引理知，t_1，t_2，t_3，t_4 至多相差 1，即它们等于 t 或 $t+1$．

同理，s_1 与 s_2 等于 s 或 $s+1$．

由于 t_1+t_2 为奇数，所以，$t_1\neq t_2$．

为确定起见，设 $t_1=t$，$t_2=t+1$．

(1) 若 $t_3=t$，因 t_3+t_4 为奇数，知 $t_4=t+1$．

则 $s_1+s_2=(t_1+t_4+s_1+s_2)-(t_1+t_4)=(t_1+t_4+s_1+s_2)-(2t+1)$ 为偶数．

于是，$s_1=s_2$．

这样一来，就有

$(t_2+s_2+t_4)-(t_1+s_1+t_3)=2$，与引理中关于线段 A_yC_y 和 D_yB_y 上的整点个数至多相差 1 的断言矛盾．

(2) 若 $t_3=t+1$，则 $t_4=t$．此时，

$s_1+s_2=(t_1+t_4+s_1+s_2)-(t_1+t_4)$

为奇数．于是，

$s_1=s$，$s_2=s+1$ 或 $s_1=s+1$，$s_2=s$．

但是，第一种情况与引理关于线段 A_xD_x 和 B_yC_y 的断言矛盾；后一种情况与引理关于线段 A_yD_y 和 B_xC_x 的断言矛盾．

解法 2 假设存在满足条件的矩形 $ABCD$.

设 $AB\geqslant\sqrt{2}$. 分别在边 AB 和 CD 上截取 $BB'=CC'=\sqrt{2}$. 于是，线段 BB' 和 CC' 都恰好分别与一条纵向的方格线相交，也都恰好分别与一条横向的方格线相交. 且 $B'C'$ 可由线段 BC 平移具有整坐标的向量 $\boldsymbol{BB'}$ 来得到. 因此，矩形 $AB'C'D$ 仍然满足条件.

继续进行这样的操作，最终，可得到一个满足条件的矩形，其各边长都小于 $\sqrt{2}$（仍记作 $ABCD$）.

此时，矩形的每条边都恰好与一条方格线相交，即或者与一条纵向方格线相交，或者与一条横向方格线相交.

设矩形的最靠左的顶点为 A，最靠下的顶点为 B，最右的顶点为 C，最上的顶点为 D. 若线段 AB 与 BC 都与纵向方格线相交，则折线 CDA 也与这些方格线相交，且它们都不与横向方格线相交. 此时，矩形 $ABCD$ 在水平方向的投影长度就大于 1（在 A 与 C 之间至少有两条纵向方格线），而在竖直方向的投影长度却小于 1，这是不可能的.

若 AB 与 BC 都与（同一条）横向方格线相交，则矩形 $ABCD$ 被夹在两条相邻的纵向方格线之间. 此时，AD 和 DC 也都与横向方格线相交，根据同样的理由，这也是不可能的.

现只剩下一种情况（或其对称情况），即 AB 与 CD 都与同一条纵向方格线 v 相交，而 BC 与 AD 都与同一条横向方格线 h 相交. 此时，点 A 与点 B 位于 h 的下方，点 C 位于 h 的上方，因此，$BC>AB$. 同理，点 B 与点 C 位于 v 的右侧，点 D 位于 v 的左侧，从而，$BC<CD$. 于是，$AB<BC<CD$，这是不可能的.

参考文献

1. 中国数学奥林匹克委员会，南开大学数学系．世界数学奥林匹克解题大辞典数论卷［M］．石家庄：河北少年儿童出版社，2002.
2. 单墫主编．初等数论［M］．南京：南京大学出版社，2000.
3. 熊全淹．初等整数论［M］．武汉：湖北教育出版社，1985.
4. 边红平主编．初等数论［M］．杭州：浙江大学出版社，2007.
5. 冷岗松，沈文选等．奥林匹克数学中的代数问题［M］．长沙：湖南师范大学出版社，2004.
6. 2003 年 IMO 中国国家集训队教练组．数学奥林匹克试题集锦［M］．上海：华东师范大学出版社，2003.
7. 2004 年 IMO 中国国家集训队教练组，选拔考试命题组．数学奥林匹克试题集锦［M］．上海：华东师范大学出版社，2004.
8. 2005 年 IMO 中国国家集训队教练组，选拔考试命题组．数学奥林匹克试题集锦［M］．上海：华东师范大学出版社，2005.
9. 2006 年 IMO 中国国家集训队教练组．数学奥林匹克试题集锦［M］．上海：华东师范大学出版社，2006.
10. 2007 年 IMO 中国国家集训队教练组．数学奥林匹克试题集锦［M］．上海：华东师范大学出版社，2007.
11. 2008 年 IMO 中国国家集训队教练组．数学奥林匹克试题集锦［M］．上海：华东师范大学出版社，2008.
12. 熊斌，田廷产．国际数学奥林匹克研究［M］．上海：上海教育出版社，2008.
13. 中等数学（2004 年增刊）．天津：天津师范大学，2004.
14. 中等数学（2005 年增刊）．天津：天津师范大学，2005.
15. 中等数学（2006 年增刊）．天津：天津师范大学，2006.
16. 中等数学（2007 年增刊）．天津：天津师范大学，2007.
17. 中等数学（2008 年增刊）．天津：天津师范大学，2008.
18. 冯跃峰．完全平方数［J］．中等数学，2008（10，11）：5—7.
19. 胡生森．裴蜀定理的应用［J］．中等数学，2004（3）：5—7.
20. 沈文选．3 的剩余类及应用［J］．中等数学，1991（3）：5—8.
21. 沈文选．整数整除问题的若干证法［J］．数学园地，1985（a）：3—4.
22. 沈文选．整数的多项式表示及整除性［J］．湖南数学通讯，1990（3）：32—35.
23. 沈文选．整数的分类、分解及末位数［J］．湖南数学通讯，1990（4）：32—35.

奥赛经典

高级教程系列

- 数学奥林匹克教程
- 物理奥林匹克教程
- 物理奥林匹克实验教程
- 化学奥林匹克教程
- 化学奥林匹克实验教程
- 生物奥林匹克教程
- 生物奥林匹克实验教程
- 信息学奥林匹克教程·基础篇
- 信息学奥林匹克教程·提高篇
- 信息学奥林匹克教程·语言篇
- 信息学奥林匹克教程·数据结构篇

初中教程系列

- 初中数学奥林匹克实用教程　第一册
- 初中数学奥林匹克实用教程　第二册
- 初中数学奥林匹克实用教程　第三册
- 初中数学奥林匹克实用教程　第四册

解题金钥匙系列

- 初中数学　　高中数学
- 初中物理　　高中物理
- 初中化学　　高中化学
- 高中生物　　高中信息学

专题研究系列

- 奥林匹克数学中的代数问题
- 奥林匹克数学中的几何问题
- 奥林匹克数学中的组合问题
- 奥林匹克数学中的数论问题
- 奥林匹克数学中的真题分析

热点专题系列

- 初中数学竞赛热点专题
- 初中物理竞赛热点专题
- 初中化学竞赛热点专题
- 初中生物竞赛热点专题
- 高中数学竞赛热点专题
- 高中物理竞赛热点专题
- 高中化学竞赛热点专题
- 高中生物竞赛热点专题

典型试题系列

- 数学奥林匹克典型试题剖析
- 物理奥林匹克典型试题剖析
- 化学奥林匹克典型试题剖析
- 信息学奥林匹克典型试题剖析

分级精讲与测试系列

- 初一数学　　初二数学
- 初三数学　　初二物理
- 初三物理　　初三化学
- 高一数学　　高二数学
- 高一物理　　高二物理
- 高一生物　　高二生物
- 高一化学　　高二化学

组　　稿＝翁李明　廖小刚
责任编辑＝翁李明
装帧版式＝周惠东

定价：38.00元


ISBN 978-7-5648-0036-9
9 787564 800369 >